U.S. Department of Justice

Federal Bureau of Investigation
Washington, D.C. 20535

June 8, 2016

MS. ALEXA O'BRIEN
MUCKROCK NEWS
DEPT MR 17650
POST OFFICE BOX 55819
BOSTON, MA 02205-5819

FOIPA Request No.: 1329073-000
Subject: Carnivore

Dear Ms. O'Brien:

Records responsive to your request were previously processed under the provisions of the Freedom of Information Act. Enclosed is one CD containing 605 pages of previously processed documents and a copy of the Explanation of Exemptions. Please be advised, these are the only copies of these documents located in our possession. The original copies of these documents could not be located for reprocessing.

Additional records potentially responsive to your subject exist. The Federal Bureau of Investigation (FBI) has located approximately 1,594 pages total of records potentially responsive to the subject of your request. By DOJ regulation, the FBI notifies requesters when anticipated fees exceed $25.00.

If all potentially responsive pages are released on CD, you will owe $40.00 in duplication fees (3 CDs at $15.00 each, less $5.00 credit for the first CD). Releases are made on CD unless otherwise requested. Each CD contains approximately 500 reviewed pages per release. The 500 page estimate is based on our business practice of processing complex cases in segments.

Should you request that the release be made in paper, you will owe $79.70 based on a duplication fee of five cents per page. See 28 CFR §16.10 and 16.49.

If you agree to receive all responsive material on CD, you will receive a $5.00 credit towards your first interim CD. As a result, we must notify you there will be a $25.00 charge when the second interim release is made in this case. At that time you will be billed for the $10.00 remaining from the $15.00 free of the first release, as well as the $15.00 duplication fee for the second release, for a total of $25.00.

Please remember this is only an estimate, and some of the information may be withheld in full pursuant to FOIA/Privacy Act Exemptions(s). Also, some information may not be responsive to your subject. Thus, the actual charges could be less.

ADDITIONAL CARNIVORE DOCUMENTS

FROM

OFFICE OF GENERAL COUNSEL
FRONT OFFICE
(THROUGH 7/28/00)

PAGES REVIEWED: 154

PAGES RELEASED: 154

EXEMPTIONS CITED: b6-1, b7C-1,
b6-3 & b7C-3

You may file an appeal by writing to the Director, Office of Information Policy (OIP), United States Department of Justice, Suite 11050, 1425 New York Avenue, NW, Washington, D.C. 20530-0001, or you may submit an appeal through OIP's FOIAonline portal by creating an account on the following web site: https://foiaonline.regulations.gov/foia/action/public/home. Your appeal must be postmarked or electronically transmitted within sixty (60) days from the date of this letter in order to be considered timely. If you submit your appeal by mail, both the letter and the envelope should be clearly marked "Freedom of Information Act Appeal." Please cite the FOIPA Request Number assigned to your request so that it may be easily identified.

Sincerely,

David M. Hardy
Section Chief,
Record/Information
Dissemination Section
Records Management Division

ADDITIONAL CARNIVORE DOCUMENTS

FROM

OFFICE OF GENERAL COUNSEL
FRONT OFFICE
(THROUGH 7/28/00)

PAGES REVIEWED: 154

PAGES RELEASED: 154

EXEMPTIONS CITED: b6-1, b7C-1,
b6-3 & b7C-3

THE WALL STREET JOURNAL

DATE: 2/12/00

PAGE: B-11

Internet Companies Decry FBI's E-Mail Wiretap Plan

By Nick Wingfield
And Don Clark
Staff Reporters of The Wall Street Journal

Internet-service providers and privacy advocates are concerned about the implications of a new electronic surveillance system devised by the Federal Bureau of Investigation, with some providers vowing to resist if they are asked to install it on their networks.

The FBI system, a sophisticated combination of hardware and software the agency has dubbed Carnivore, must be connected directly to an ISP's network. Once it is connected, Carnivore has the potential to keep tabs on all of the communications on the network. The FBI has said it will use the system only with valid court orders and that Carnivore will allow it to narrowly target its investigations.

However, ISPs, industry representatives and privacy advocates, responding to a report in The Wall Street Journal about the FBI system, criticized the potential for excessive monitoring of online communications. "We have some deep concerns as we look at this harder," said Jeff Richards, executive director of the Internet Alliance, a trade association for Internet providers that counts America Online Inc., EarthLink Inc. and WorldCom Inc.'s UUNET division among its members.

The Carnivore system is believed to be able to single out all sorts of electronic traffic of a person being investigated. Besides e-mail, that includes instant-messaging systems, visits to Web sites and Internet relay chat sessions, a form of communication favored by hackers trying to mask their identities.

It isn't clear, however, whether Carnivore can overcome some of the sophisticated scrambling systems that have been developed for the Internet. Scrambling data to make it hard to read is an obvious response for people worried about their messages being caught up in the FBI vacuum cleaner. Such data-scrambling wouldn't necessarily prevent the FBI from knowing the message's destination, security experts said.

To better protect their cyber-trails, users would have to seek services designed to protect anonymity on the Internet. For example, Zero-Knowledge Systems, Montreal, sells users online pseudonyms for use when conducting business online.

Critics of the FBI system fear Internet-service providers will have little guarantee that Carnivore is doing only what the FBI says it is doing. Because the FBI seems to need little assistance in running the system, technicians for the ISPs can't do much to monitor whether FBI agents are limiting their investigations to an individual named in a court order.

"The FBI takes the position of, 'Trust us, we're the government. Open your entire network to us,' " says Barry Steinhardt, associate director for the American Civil Liberties Union, which sent a critical letter about Carnivore to members of Congress. "There's no way for an ISP to know what they're doing."

One ISP that hadn't been contacted by the FBI about Carnivore said it normally complies with court orders from law-enforcement agencies for the communications of specific individuals. But the ISP said it wouldn't comply with an order to install Carnivore on its network.

"I would have to say we would fight such a court order," said Ehud Gavron, the chief technology officer of RMI.Net Inc., an ISP based in Denver with 110,000 subscribers. "We would not want the privacy of all users to be compromised on the basis of witch hunts for one user."

The FBI argues that state and federal judges closely scrutinize its wiretapping activities and that the product of any telephone or Internet intercept must be open to outside audit. The bureau says that it developed the Carnivore system precisely to address the same privacy concerns that many Internet providers have. FBI technicians also have tried in recent weeks to explain to industry specialists how Carnivore works, partly to allay fears that the system might be open to abuse.

Still, there is a drive afoot in the Internet industry to create a more open solution that could replace Carnivore. Industry experts argue that creating their own device would lessen suspicions and allow for quicker modifications as Internet protocols change. The FBI says that a small number of Internet providers already have built-in capacities to meet federal wiretap requests. Carnivore is required for those that don't have the ability to do the wiretaps themselves.

—Neil King Jr. contributed to this article.

Journal Link: Read an issue briefing and join a discussion about privacy and the Internet in the online Journal at **WSJ.com**.

8

Doc # 1

The Washington Post

DATE: 7-12-00

PAGE: E-1

FBI Internet Wiretaps Raise Issues Of Privacy

New System Tracks Suspects Online

By John Schwartz
Washington Post Staff Writer

The FBI has deployed an automated system to wiretap the Internet, giving authorities a new tool to police cyberspace but drawing concerns among civil libertarians and privacy advocates about how it might be used.

The new computer system, dubbed "Carnivore" inside the FBI because it rapidly finds the "meat" in vast amounts of data, was developed at FBI computer labs in Quantico, Va., and has been used in fewer than 50 cases so far.

But that number is sure to rise, said Marcus Thomas, chief of the FBI's cyber-technology section at Quantico. "In criminal situations there's not yet been a large call for it," he said, but the bureau already has seen "growth in the rate of requests."

Civil liberties groups said the new system raises troubling issues about what constitutes a reasonable search and seizure of electronic data. In sniffing out potential criminal conduct, the new technology also could scan private information about legal activities.

"It goes to the heart of how the Fourth Amendment and the federal wiretap statute are going to be applied in the Internet age," said Marc Rotenberg, head of the Washington-based Electronic Privacy Information Center.

The new system, which operates on off-the-shelf personal computers, takes advantage of one of the fundamental principles of the Internet: that virtually all such communications are broken up into "packets," or uniform chunks of data. Computers on the Internet break up e-mail messages, World Wide Web site traffic and other information into pieces and route the packets across the global network, where they are reassembled on the other end.

FBI programmers devised a "packet sniffer" system that can analyze data flowing through computer networks to determine whether it is part of an e-mail message or some other piece of Web traffic.

The ability to distinguish between packets allows law enforcement officials to tailor their searches so that, for example, they can examine e-mail but leave alone a suspect's online shopping activities. The system could be tuned to do as little as monitoring how many e-mail messages the suspect sends and to whom they are addressed—the equivalent of a telephone "pen register," which takes down telephone numbers being called without grabbing the content of those calls.

"That's the good news," said James Dempsey, an analyst with the Center for Democracy and Technology, a Washington high-tech policy group. "It is a more discriminating device" than a full wiretap, he said.

But Dempsey expressed worries about the new system, which would be installed at the offices of a suspect's Internet service provider. Just as the device could be used to fine-tune a search, it also could used for broad sweeps of data. "The bad news is that it's a black box the government wants to insert into the premises of a service provider. Nobody knows that it does what the government claims it would do," Dempsey said.

Existence of the Carnivore system was discussed in a Wall Street Journal article yesterday, which reported that the FBI showed the system to telecommunications industry experts two weeks ago.

Albert Gidari, a lawyer who works for the wireless industry, was present at the FBI demonstration. He said the FBI's announcement was intended to counter industry assertions that it would be very difficult to provide the kind of pen-register wiretap capability that the agency wants.

Since the demonstration, Gidari said, one faction within the telecommunications industry was pleased with the FBI's efforts. But Gidari said the other faction was saying: "Wait a minute—what are the liability issues? What are the privacy issues? We don't want third-party software on our system."

Although Congress has passed legislation requiring telephone companies to make their developing high-tech networks easy to wiretap, Gidari is one of a large number of industry experts who believe the law does not apply to wiretapping the Internet. "The FBI overreaches in everything they do," said Gidari, who is president of G-Savvy, an Internet consulting company.

A former federal prosecutor sounded a more supportive tone. "If what it does is it helps comply with wiretaps, and it helps minimize what you're getting—to help get what the court authorizes you to get—there's nothing wrong with it," said Mark Rasch, now a security consultant with Reston-based Global Integrity.

Still, Rasch said the technology raised questions that have yet to be fully explored by law enforcement. The PC robocop examines all packets coming through a computer network but gives live law enforcement officers only those packets related to the subject of the investigation.

"The stuff that is examined only by a computer and not by a human being—was that information searched?" Rasch asked. He then suggested an answer: "It is a search, but it is to an extent less invasive than it would be if you did not use this technology."

The first news of Carnivore actually came in April during congressional testimony by Washington lawyer Robert Corn-Revere, who represented an Internet service provider that tried to resist attaching the system to its network. Corn-Revere suggested that such a system could be used to track dissidents and journalists online. "There are some human rights issues here," he said.

But Thomas of the FBI said there is nothing mysterious about the new device. "This is an effort on the FBI's part to keep pace with changes in technology—to maintain our ability" to lawfully intercept everything from pen-register data to full wiretaps with court authorization. "It's not an increase in our authority; it doesn't present a change of volume in what we do," he said.

DOC. #2

Los Angeles Times

DATE: 7-14-
PAGE: A-16

Justice, on Both Sides of the Border

Agustin Vazquez Mendoza landed on the FBI's 10 most wanted list four years ago for allegedly ordering his henchmen to kill a Drug Enforcement Administration agent in Arizona. Now he's under arrest, but in Mexico, which must decide whether to extradite a Mexican citizen to face charges in the United States. Mexican law officers mounted a nationwide manhunt to capture Vazquez and certainly want him brought to justice, but some traffickers have won appeals against extradition.

Most countries are understandably reluctant to hand over a citizen to be tried in a foreign country. In addition, the language in the current Mexico-U.S. treaties clearly specifies that neither country is bound to extradite a citizen. However, there are circumstances in the Vazquez case that should make it easier for Mexico to send him off.

Since President Ernesto Zedillo took office, there has been a shift of attitude in Mexico on extradition. At least nine Mexican suspects have been sent to be tried in the United States. In two of those cases, the suspects allegedly killed U.S. immigration officials, inviting comparison with the Vazquez case.

According to U.S. authorities, Vazquez ordered the murder of agent Richard Fass in order to keep both a drug delivery and the $160,000 the undercover agent was about to pay for it.

Perhaps the most persuasive argument is that Vazquez, who fled to Mexico after the killing, is not accused of a crime in Mexico and if he is not extradited will have to be set free. Mexico's foreign minister should consent to the U.S. extradition request and petition the justice system to send him north as quickly as the legal process allows.

46

Doc. #3

THE WALL STREET JOURNAL

DATE: 7/14/02
PAGE: A16

EarthLink Says It Won't Install Device for FBI

One of the nation's largest Internet service providers, EarthLink Inc., has refused to install a new Federal Bureau of Investigation electronic surveillance device on its network, saying technical adjustments required to use the device caused disruptions for customers.

The FBI has used Carnivore, as the surveillance device is called, in a number of criminal investigations. But EarthLink is the first ISP to offer a public account of an actual experience with Carnivore. The FBI has claimed that Carnivore won't interfere with an ISP's operations.

By Wall Street Journal staff reporters Nick Wingfield, Ted Bridis and Neil King Jr.

"It has the potential to hurt our network, to bring pieces of it down," Steve Dougherty, EarthLink's director of technology acquisition, said of Carnivore. "It could impact thousands of people."

While EarthLink executives said they would continue to work with authorities in criminal investigations, they vowed not to allow the FBI to install Carnivore on the company's network. The company also has substantial privacy concerns.

EarthLink has already voiced its concerns in court. The ISP is the plaintiff in a legal fight launched against Carnivore earlier this year with the help of attorney Robert Corn-Revere, according to people close to the case. Previously, the identity of the plaintiff in the case, which is under seal, wasn't known. A federal magistrate ruled against EarthLink in the case early this year, forcing it to give the FBI access to its system. Mr. Corn-Revere declined to comment.

EarthLink's problems with Carnivore began earlier this year, when the FBI installed a Carnivore device on its network at a hub site in Pasadena, Calif. The FBI had a court order that allowed it to install the equipment as part of a criminal investigation.

The FBI connected Carnivore, a small computer box loaded with sophisticated software for monitoring e-mail and other online communications, to EarthLink's remote access servers, a set of networking equipment that answers incoming modem calls from customers. But Carnivore wasn't compatible with the operating system software on the remote access servers. So EarthLink had to install an older version of the system software that would work with Carnivore, according to Mr. Dougherty.

EarthLink says the older version of the software caused its remote access servers to crash, which in turn knocked out access for a number of its customers. Mr. Dougherty declined to specify how many, saying only that "many" people were affected.

EarthLink executives said they were also concerned about privacy. The company said it had no way of knowing whether Carnivore was limiting its surveillance to the criminal investigation at hand, or was trolling more broadly. Other ISPs have said there could be serious liability issues for them if the privacy of individuals not connected to an investigation is compromised.

"There ought to be some transparency to the methods and tools that law enforcement is using to search-and-seize communications," said John R. LoGalbo, vice president of public policy at PSINet Inc., an ISP in Ashburn, Va.

EarthLink executives declined to say whether the company has received court orders for information about other customers since the disruption earlier this year. EarthLink said it would help authorities in criminal investigations using techniques other than Carnivore.

The FBI insists that Carnivore doesn't affect the performance or stability of an Internet provider's existing networks. The bureau says Carnivore passively monitors traffic, recording only information that is relevant to FBI investigations.

In some cases, the FBI said, the Internet provider is equipped to turn over data without the use of Carnivore. This is common in cases where only e-mail messages are sought because that type of data can easily be obtained through less-intrusive means.

Attorney General Janet Reno said yesterday that she was putting the system under review. She said the Justice Department would investigate Carnivore's constitutional implications and make sure that the FBI was using it in "a consistent and balanced way."

47

Doc. #4

Parkinson
Ken
from: John E. Collingwood

White House Proposes Wiretap Law

By KALPANA SRINIVASAN
(c) The Associated Press

WASHINGTON (July 17) - The White House proposed legislation Monday to update wiretapping rules so that legal protections currently applied to telephone calls are extended to electronic communication, such as e-mail.

The plan would require law enforcement officials to obtain high-level approval before applying for a court order to intercept the content of e-mail - in line with current rules that govern listening to phone calls.

"Basically, the same communication, if sent different ways - through a phone call or a dial-up modem - is subject to different and inconsistent privacy standards," said White House Chief of Staff John Podesta, in announcing the proposals. "It's time to update and harmonize our existing laws to give all forms of technology the same legislative protections as our telephone conversations."

The measure also addresses so-called "trap and trace" orders which allow law enforcement officials to identify the source of a phone call or an e-mail, but not intercept its content. Under the proposal, law enforcement officials would only need one order to trace an e-mail or a phone call, even though such communications may travel through multiple phone carriers or Internet providers.

Officials also could trace such communications without prior approval in an emergency situation, such as when a computer is under attack.

But for the first time, the administration is proposing that a federal or state judge independently determine whether the facts support such a trace order. Under current rules, judges accept the declaration of law enforcement officials agencies that such an order is warranted.

Those changes could affect the new "Carnivore" system, which the FBI is using to obtain e-mails of investigative subjects after getting a search warrant. When Carnivore is placed at an Internet service provider, it scans all incoming and outgoing e-mails for messages associated with the target of a criminal probe.

Under the proposed changes, if the Carnivore system is being used to intercept the content of electronic communications, then law enforcement officials would first need high-level Justice Department approval before obtaining a court order, Podesta said. Higher standards limiting its use also would apply, he said. If Carnivore is being used only to track information, officials would need an independent judge to review the tracing order, he added.

But the American Civil Liberties Union chided the administration's proposals Monday, saying it should have suspended use of the system outright.

"Carnivore represents a grave threat to the privacy of all Americans by giving law enforcement agencies unsupervised access to a nearly unlimited amount of communications traffic," said Barry Steinhardt, ACLU associate director.

Last week, ACLU officials said they were going to use the Freedom of Information Act to try to force the FBI to disclose details of the inner workings of Carnivore.

The proposed measures would also address inconsistencies in how current law applies to different networks carrying Internet traffic. For example, now that cable systems are being upgraded to offer two-way services, laws that apply to dial-up modems over phone lines should be extended to cable connections, Podesta said.

The proposal requires congressional approval, and several lawmakers already have introduced their own versions.

The Clinton administration also announced Monday updates to its export control policy for powerful data and voice-scrambling technology. Under the change, American companies can sell encryption products to any end user in the European Union or these eight other trading partners: Australia, Norway, Czech Republic, Hungary, Poland, Japan, New Zealand and Switzerland. The policy change will also remove a previous technical review waiting period of 30 days.

AP-NY-07-17-00 1458EDT

Doc #5

TOTAL P.01

WALL STREET JOURNAL

DATE 7/17/00
PAGE B7

ACLU Asks Details On FBI's New Plan To Monitor the Web

By Nick Wingfield
Staff Reporter of The Wall Street Journal

The American Civil Liberties Union is seeking to force the Federal Bureau of Investigation to disclose the technical details behind a controversial electronic surveillance system created by the bureau.

The ACLU, using a novel tactic to identify the monitoring capabilities of the system, filed a Freedom of Information Act request with the FBI Friday, asking the bureau to release the computer "source code" for Carnivore, as the surveillance system is called. The civil-liberties group also requested that the FBI turn over "letters, correspondence, tape recordings, notes, data, memoranda, e-mail" and other information connected with Carnivore. The ACLU also asked for information related to Omnivore and EtherPeek, two other surveillance systems used in the past by the bureau.

The request reflects the growing concern among privacy groups and Internet companies about the privacy implications of Carnivore. The FBI surveillance system, a hardware device that contains a specialized program for tracking e-mail and other forms of online communication, has especially raised hackles among Internet service providers. The FBI is attempting to install Carnivore on the networks of ISPs as part of specific criminal investigations of online users. But ISPs say they have no way of knowing whether Carnivore is limiting the scope of its surveillance to the cases at hand.

As a result, critics of Carnivore have called on the government to reveal the technical capabilities of the system. Such information could indicate whether Carnivore is able to restrict its monitoring to the communications of, say, a single criminal suspect while ignoring other data traffic irrelevant to the investigation.

The source code behind Carnivore could provide clues to those capabilities. Source code is essentially the technical blueprint behind a program. The ACLU contends, and technical experts concurred, that examining the source code behind Carnivore's proprietary surveillance software could reveal something of the inner workings of the system.

The Electronic Privacy Information Center, a Washington advocacy group, last week also filed a sweeping Freedom of Information request for "all records" relating to Carnivore, though it didn't explicitly request the system's source code. "But we made clear we are seeking everything, including software," said David Sobel, a privacy activist at the center.

It is unclear whether using the Freedom of Information Act will compel the FBI to produce the software behind Carnivore though. Requests made under the act are normally used to obtain official government documents, not software code. Barry Steinhardt, associate director of the ACLU, said two federal appeals-court rulings that classified software code as a form of speech could help his case.

"I am all but certain they will not want to release any information on Carnivore, and we will probably have to fight this in the courts," Mr. Steinhardt said of the FBI. "But we think this is worth fighting for."

The FBI didn't return calls seeking comment on the Freedom of Information request.

As the outcry against Carnivore has escalated, some prominent figures in the Internet industry have expressed a somewhat more sympathetic view toward the FBI. Vint Cerf, who has been dubbed the "father of the Internet" for his development of the early technical foundations of the network, said it is "understandable that law-enforcement agencies feel pressed to develop methods to observe Internet traffic for the same reasons they have felt compelled to find ways to listen to certain telephone conversations."

But Mr. Cerf, in an e-mail message, added that such modern surveillance techniques need to be balanced "against potentially abusive practices that could seriously erode personal privacy"

—Neil King Jr. contributed to this article.

Coca-Cola Files to Have Second Race-Bias Suit Moved to Federal Court

By a Wall Street Journal Staff Reporter

ATLANTA—Coca-Cola Co., in the process of settling a class-action race-discrimination lawsuit, has filed a motion to move a second, $1.5 billion race-bias suit to federal from state court.

The soft-drink company argued in a motion filed Friday that most of the claims in the lawsuit, filed last month on behalf of four female black Coke employees by Willie E. Gary and Johnnie Cochran, involve federal laws.

But a lawyer on Mr. Gary's team, Tricia C.K. Hoffler, disagreed and said Mr. Gary would file a motion this week to keep the case in state court. Mr. Gary, a personal-injury attorney, generally brings his cases to state courts and has said he prefers that venue.

The lawsuit filed by Mr. Gary claims a variety of forms of discrimination, including negligent hiring, intentional infliction of emotional harm and hostile work environment. Coke has called Mr. Gary an opportunist and denied the charges.

Doc. #6

DATE 10/22
PAGE E1

WASHINGTON

U.S. Hopes to Extend Online Wiretapping

By John Schwartz
Washington Post Staff Writer

The Clinton administration yesterday called for updating wiretapping laws to extend the powers of law enforcement to the online world while providing new legal protections for electronic communication.

Administration officials also announced, as expected, a plan to loosen controls on the export of encryption software—the programs that help Internet users scramble messages and data to protect them from prying eyes.

On the wiretapping issue, White House chief of staff John D. Podesta, in a speech at the National Press Club, described the coming legislative package as seeking to eliminate confusion about the level of legal protection for various forms of communication.

Telephone conversations get fairly strong protection from federal wiretaps under the 1968 Crime Patrol and Safe Streets Act, which required a court order and high-level Justice Department approval. Wiretape rules for e-mail sent by dial-up modem are covered by the Electronic Communications Privacy Act of 1986. That law might not cover e-mail sent by high-speed cable modem, and cable companies have argued that their online services should be given extremely high protection from government surveillance under the Cable Act.

"It's time to update and harmonize our existing laws to give all forms of technology the same legislative protections as our telephone conversations," Podesta said.

Lawmakers said they welcome the opportunity to work with the administration on these issues. Sen. Orrin G. Hatch (R-Utah), who has introduced an Internet privacy bill, said: "It is imperative that we balance the interests of law enforcement with the privacy rights of the American people. We must ensure that appropriate checks are in place where the government accesses private communications of Americans."

Podesta said the bills making up the package would be unveiled within 10 days, and that he hopes the legislation can be passed by the end of the year.

Podesta also spoke about the new surveillance technology known as Carnivore, which gives law enforcement authorities the ability to selectively monitor the Internet traffic of individuals, similar to the devices that can record the telephone numbers of calls made and received by a suspect. Unlike full-fledged wiretaps, the judicial oversight of such surveillance is slight, and the protection against abuses of the technology by law enforcement is weak. Podesta called for greater judicial oversight.

The Podesta speech was not well received by civil liberties advocates, who have fought Carnivore and other administration attempts to expand wiretapping capabilities on the Internet. Barry Steinhardt, associate director of the American Civil Liberties Union, called the speech "deeply disappointing. . . . While the Clinton administration's proposals have some heartening qualities to them, they are too little and too late," with too little time in the legislative session to pass new bills. The Carnivore system, Steinhardt said, "represents a grave threat to the privacy of all Americans by giving law enforcement agencies unsupervised access to a nearly unlimited amount of communications traffic."

Podesta also discussed the new encryption policy, which the administration can implement immediately. Under the plan, U.S. companies will be able to export sophisticated cryptography products to users in any nation in the European Union and to Australia, Norway, the Czech Republic, Hungary, Poland, Japan, New Zealand and Switzerland. The government will eliminate the statutory 30-day waiting period before such exports can take place but will keep in place a requirement that new technologies be submitted to the government for a technical review.

Encryption has been a high-tech battlefield from the early days of the Clinton administration. Few technologies are as important in the fight to maintain personal and business privacy, but few technologies present such daunting issues for law enforcement officials like FBI Director Louis J. Freeh, who often warns that criminals and terrorists can use "crypto" to cloak their plans and activities. High-tech companies successfully argued that U.S. restrictions harmed only American companies, since overseas firms were successfully marketing strong encryption products, and in January the Clinton administration reduced controls on encryption exports.

"The reducing of these regulations will certainly allow U.S. software makers to compete in the global marketplace," said Robert Holleyman, the chief executive of the Business Software Alliance.

Doc #7

WALL STREET JOURNAL

DATE 7/19/00
PAGE A22

'Carnivore' Won't Devour Cyber-Privacy

By Bruce Berkowitz

On Monday the White House proposed new legislation regulating surveillance by law enforcement agencies on the Internet. But civil libertarians are already complaining that this plan does little to address the problems ostensibly raised by Carnivore, the FBI's new software system for performing court-ordered wiretaps at Internet service providers (ISPs).

Using a laptop computer, law enforcement officials can hook Carnivore into an ISP's network. Once installed, it reads the headers of each e-mail message—listing the sender, recipient and subject of the message—as it passes through. If the sender or recipient is the target of a tap, Carnivore records the message.

Rights at Risk?

Here's the rub: Before Carnivore can know whether a message belongs to a targeted party, it must browse the headers of all the messages passing through the ISP. With a traditional phone tap, law enforcement officers only listened to the telephone line that the subject of the tap was using. The ACLU and other critics complain that when Carnivore reads the headers of anyone who is not a target it violates their rights.

The ACLU and other Carnivore critics need to get a grip—and a better understanding of the new technology.

Unlike old-fashioned analog telephone calls, e-mail messages are transmitted digitally. A computer slices and dices the message into packets, each with an identifying tag. The packets then spread out throughout the Internet, finding the most efficient path to the destination. When they arrive, they are reassembled, and the recipient gets the message. As a result, with e-mail, you cannot "tap a line" because often there is, literally, no particular line to tap. All you can do is scan the messages that pass through a link a suspect is known to use—like his ISP—and pick out the ones that belong to him. That's what Carnivore does.

The ACLU complains that using a computer to monitor an ISP system would collect vast amounts of innocent data. But what do they expect the feds to use—a typewriter and an abacus? Note to FBI: Hire a public relations firm, and name your next project "Vegetarian."

These kinds of flaps are happening more and more often. Last April some privacy advocates complained when the FBI requested $15 million for "Digital Storm," a program for monitoring telephone calls and analyzing recordings. In September, a programmer in North Carolina found the notation "NSA Key" in a Microsoft software patch. Soon rumors bounced through the Internet claiming Windows had a back door that allows the National Security Agency to monitor your computer. (Microsoft explained that the tag merely signified that the software complied with the agency's security standards.)

The granddaddy of all bogus fears, though, is Echelon. If you believe some European Union parliamentarians, the United States and Britain operate an international network that monitors virtually all communications, and extracts choice nuggets with powerful computers that recognize key phrases in messages like "assassination," "terrorist attack" or "industrial secret."

In reality, it's not easy to find a specific message in a flood of free-flowing digital data. That's the whole reason for getting a court order for a wire tap. If you cannot hook into an ISP, you have to do a lot of searching to find the message you want to intercept.

That is also why the European campaign against Echelon is so quixotic. True, the folks at NSA intercept communications and they have powerful computers and ingenious software that helps with the processing. But it is impossible for even the best computer system to routinely sort through all of the world's telecommunications and pull out telltale messages, as the Echelon paranoids would have you believe.

> Usually you need to know what you are looking for and where the message might appear before you have much of a chance of finding it. Also, the cases in which one message tells a whole story are rare. Good law enforcement and intelligence usually requires multiple sources and collateral information to make sense of an intercept.
>
> The privacy advocates have the story reversed. It's getting harder, not easier, for our law enforcement and intelligence organizations to listen in on communications. In the old days you could tap a line or intercept a microwave link. It's much more difficult to capture digital messages that pass over fiber optics or bounce through cellular networks. And, with strong encryption software freely available world-wide, anyone really determined to keep a message secret can usually do so.
>
> If you have any doubts, just recall how many intelligence surprises we have had lately—the Indian nuclear test, the North Korean missile test, the terrorist bombings of American targets in the Mideast and Africa. Part of the problem is that we cannot get to many of the sources that we used to, and everyone is getting better at concealing their communications.

So why is it so easy to stir up these controversies about privacy? The simple fact is that relations between the government and the new information industries are lousy. There is too much suspicion and too little communication.

The administration gets part of the blame for its ham-handed policies. Carnivore is a good example. A lot of controversy could have been defused if the FBI had offered more insight into how the system worked and how the rights of non-suspects would be protected.

But the record of the technogeeks has not been much better. They often act as though law enforcement officials have no business poking into their activities at all—as though one could stop international computer criminals with a good neighborhood watch program.

It's all too easy to lose sight of the fact that Carnivore's main targets are cybercriminals—in other words, the kinds of crooks who are a plague on the Internet and target dot-com companies. Growth rates for Internet shopping have been slipping lately. According to some experts, people worry about whether their credit card numbers and health records are safe. You would think that e-business would be the first to support better law enforcement on the net.

Common Goals

All the good guys in this dispute have common goals. Defense and intelligence officials want to protect the nation's communications infrastructure. Law enforcement officials want to chase crooks, and companies want the cops to catch them. Consumers want privacy. The path to all is the same: secure information systems.

Doc. #8

2

reasonable cooperation from the private sector, and aggressive law enforcement and effective intelligence closely monitored by responsible public officials.

Fixing the relationship between Washington and Silicon Valley needs to be a top priority for the next administration. The only people benefitting from controversies like the one over Carnivore are terrorists, criminals and rogue states.

Mr. Berkowitz is a research fellow at the Hoover Institution and coauthor of "Best Truth: Intelligence in the Information Age" (Yale University Press, 2000).

July 19, 2000

Honorable Charles T. Canady
Chairman
Subcommittee on the Constitution
Committee on the Judiciary
House of Representatives
Washington, D.C. 20515

Dear Mr. Chairman:

We very much appreciate the opportunity to appear before the Constitution Subcommittee on Monday to discuss "Carnivore." The public testimony, we believe, will be very helpful in our efforts to explain what Carnivore is and, equally important, what it is not.

In that regard, *USA Today* asked us to provide a brief 350 word explanation for use on the editorial page. While a full statement obviously will be provided to the Subcommittee, we would like to share with you the text of what was provided to the newspaper. In a very concise fashion, it encapsulates our explanation of what the system does electronically to ensure strict compliance with the court orders that instruct us precisely what can and cannot be intercepted. I also have enclosed a graphic that you may find helpful.

As the brief summary points out, Carnivore is used only when Internet Service Providers are unable on their own to restrict interceptions within the narrow confines of the controlling court order. In addition, no interception can occur unless the FBI or other law enforcement agency can demonstrate to a judge's satisfaction that the strict statutory requirements have been met, e.g., that there is probable cause that a crime is being or has been committed, that the intercepted e-mails will be in furtherance or about that crime, and that the interceptions are necessary to collect evidence of that crime. That is why its use has been very limited, predominately to intercept e-mails in terrorism cases.

I hope you find this helpful. Again, we look forward to testifying and, in the interim, if you have any questions, please do not hesitate to ask. We would be pleased to brief on any aspect of this system.

Sincerely yours,

John E. Collingwood
Assistant Director
Office of Public and
Congressional Affairs

1 - Mr. Pickard - Rm 7142
1 - Mr. Alba - Rm 7128
1 - Mr. Gallagher - Rm 7110
1 - Mr. Garcia - Rm 7116
1 - Dr. Kerr - Rm 3090
1 - Mr. Parkinson - Rm 7427
1 - [redacted] - Rm [redacted]
JEC:mmc (25)

1 - Mr. Collingwood
1 - [redacted] 66-1
1 - [redacted] 67C-1
1 - CAO file copy

IDENTICAL LETTERS SENT TO ALL
ADDRESSES ON ATTACHED LIST

Doc. #9

Honorable Charles T. Canady

Honorable Henry J. Hyde
House of Representatives
Washington, D.C. 20515

Honorable Asa Hutchinson
House of Representatives
Washington, D.C. 20515

Honorable Spencer Bachus
House of Representatives
Washington, D.C. 20515

Honorable Robert W. Goodlatte
House of Representatives
Washington, D.C. 20515

Honorable Bob Barr
House of Representatives
Washington, D.C. 20515

Honorable William L. Jenkins
House of Representatives
Washington, D.C. 20515

Honorable Lindsey Graham
House of Representatives
Washington, D.C. 20515

Honorable Melvin L. Watt
House of Representatives
Washington, D.C. 20515

Honorable Maxine Waters
House of Representatives
Washington, D.C. 20515

Honorable Charles T. Canady

Honorable Barney Frank
House of Representatives
Washington, D.C. 20515

Honorable John Conyers, Jr.
House of Representatives
Washington, D.C. 20515

Honorable Jerrold Nadler
House of Representatives
Washington, D.C. 20515

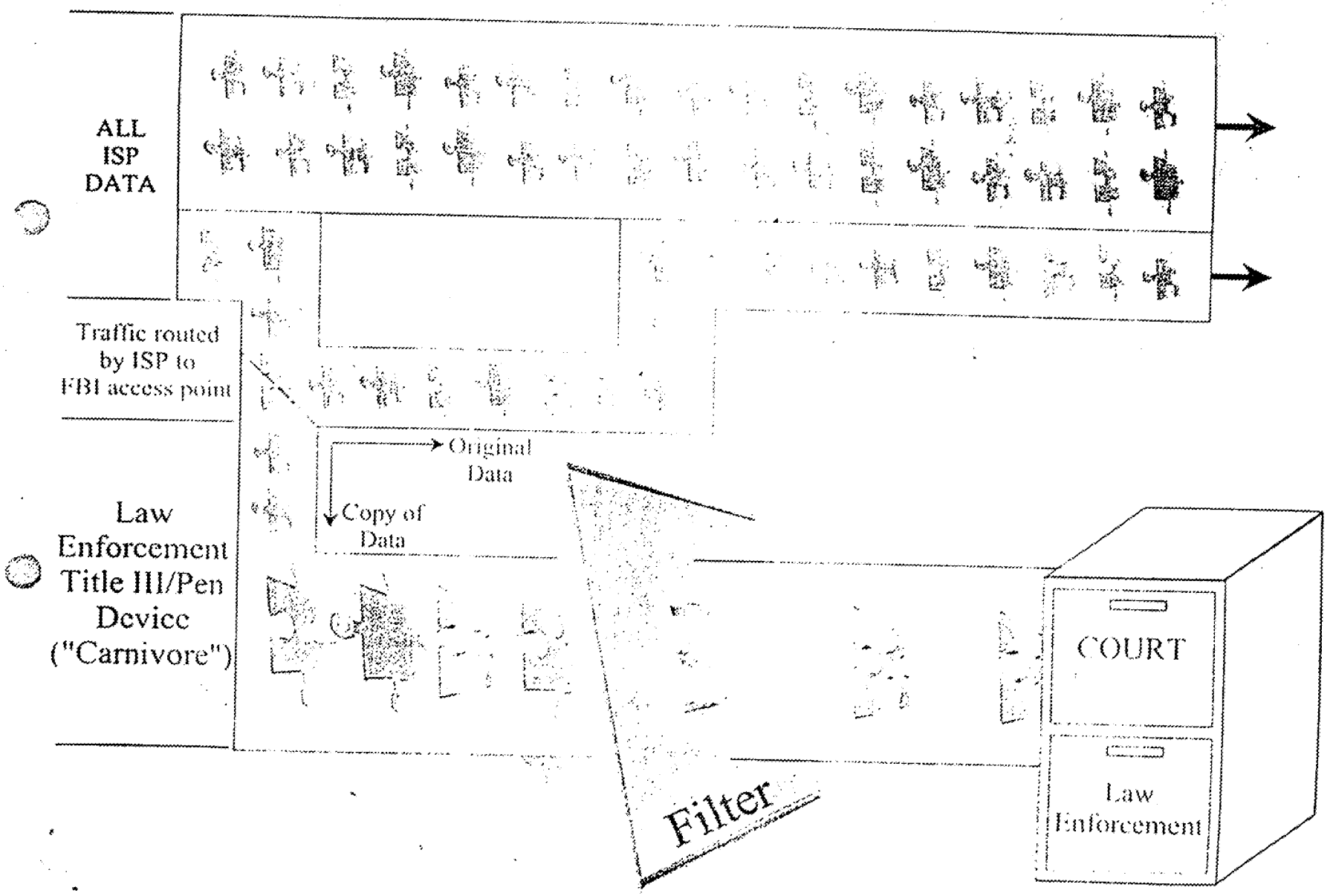
First, lets get the facts straight. The FBI and all other law enforcement agencies can only intercept e-mails pursuant to a court order signed by a judge who is satisfied that the government has demonstrated probable cause that a serious crime is being or has been committed, the e-mails will be about that crime and the interception is necessary to obtain evidence about the crime. To conduct an intercept beyond that is a federal crime subject to severe criminal and civil sanctions. The entire process requires continual reporting to a court and, of course, ultimately is subject to vigorous challenge by defense attorneys.

What does "carnivore" do? In the simplest terms, it ensures that only the exact communications authorized by the court to be intercepted are what is intercepted. So, for example, if a court authorizes only the interception of e-mail from a particular drug dealer to another drug dealer, this system captures only that e-mail to the exclusion of all other computer communications regardless of who sends them and where they are going. Nothing else is monitored or collected, and everything collected is supervised by the court. It would be a federal crime to do otherwise.

When is carnivore used? It is used only when an Internet service provider cannot, on its own, effect the interceptions consistent with a narrow court order. Accordingly, it has been used very few times, predominately to intercept e-mails in terrorism cases and, again, subject to the supervision of a court.

In 1968, Congress spelled out strict requirements for the interception of communications. Carnivore simply ensures that law enforcement complies precisely with those requirements as technology advances. We understand why certain segments oppose this court ordered technique. But since 1968, because of this law, many lives have been saved and thousands of drug dealers, terrorists, child predators and spies are in jail.

The Chairman of PSINet laid out the appropriate challenge. He does not want to see carnivore on his network unless we can prove it sifts out only the traffic from the target of a court order. That, of course, is precisely what carnivore does, electronically protecting the privacy of those not subject to the court order.


ALL ISP DATA
Traffic routed by ISP to FBI access point
Original Data
Copy of Data
Law Enforcement Title III/Pen Device ("Carnivore")
Filter
COURT
Law Enforcement

WALL STREET JOURNAL

DATE 7/20/00
PAGE A28

Carnivore E-Mail Tool Won't Eat Up Privacy, Says FBI

By Ted Bridis
And Neil King Jr.
Staff Reporters of The Wall Street Journal

WASHINGTON—Packed in a slim laptop computer, the Federal Bureau of Investigation's Internet surveillance system, Carnivore, looks downright docile. One of its creators calls it merely a "tool in a tool box" for tracking hackers and terrorists. Its name, the FBI admits, is unfortunate.

It is too late to change the name—but not too late, the FBI figures, to try to change the opinions of privacy advocates and lawmakers who have spoken harshly of the high-tech sniffer. So the agency has launched an intense, behind-the-scenes campaign to deflect congressional skepticism and convince wary Internet companies that Carnivore is a much pickier eater than its critics claim.

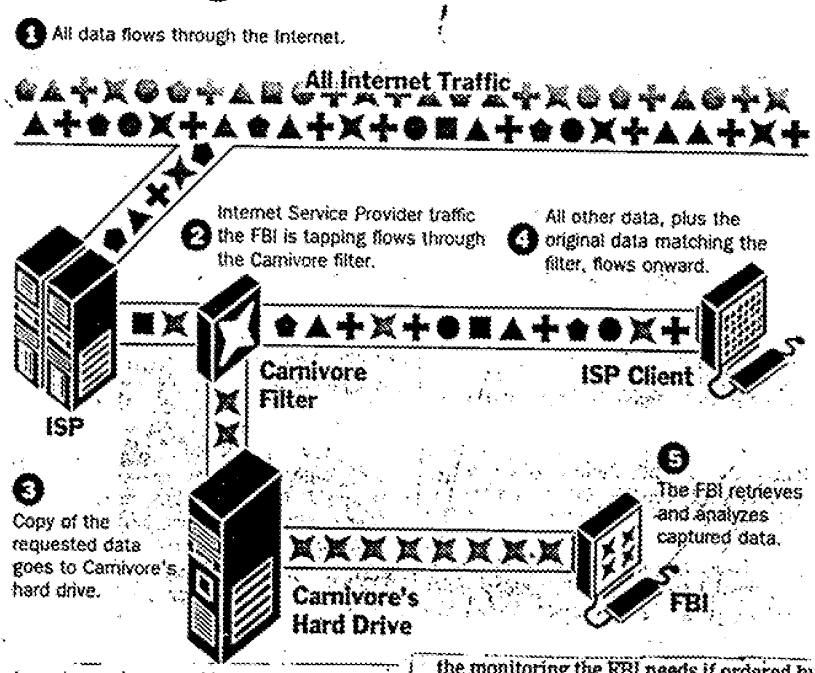
Since news of Carnivore broke last week, FBI officials have swarmed Capitol Hill to demonstrate the system to key members of Congress and their staff. The officials also have shown it to two federal judges and a small group of reporters for The Wall Street Journal. And Tuesday, the FBI published a lengthy article about Carnivore on its Web site, describing it as a "diagnostic tool" that employs new technology "to lawfully obtain important information while providing enhanced privacy protection."

The message: Carnivore is a surgical law-enforcement device used rarely and only under strict court orders. And, contrary to fears espoused publicly in recent days, the system doesn't gobble up all passing e-mail in its search for the correspondence of a single suspect. "This device is blind to everything but the packet [of information] that it's set to retrieve," says Thomas Motta, an assistant general counsel for the FBI. "It's like a cop who can't see anything but a blue car on a highway."

In advance of a hastily called congressional hearing next week, FBI officials also have been expressing regrets about the system's name. Carnivore was the in-house moniker given to the successor of an earlier surveillance system, which was called Omnivore. No one thought the name would become public. When it did last week, Attorney General Janet Reno called for a name change, and FBI Director Louis Freeh started asking how the bureau could have had such a tin ear.

"Let's just say, we're going to put names through the giggle-test a little differently in the future," says Donald Kerr, director of the special Quantico, Va., lab that developed Carnivore.

The system's critics are likely to demand more than merely cosmetic change. Lawmakers are eager to know how voracious Carnivore could get. Can it vacuum up Internet communications from innocent users? How frequently is it used, and under what legal basis? Is Carnivore hooked permanently into the country's Internet service providers? How can we trust that it does only what the FBI says?



Protecting Citizens

"We want to hear exactly how this system works and make sure it raises no constitutional problems," says Rep. Charles Canady, the Florida Republican who heads the House judiciary subcommittee that will question FBI officials next week. Adds Rep. Asa Hutchinson, an Arkansas Republican and member of the same panel: "We have to protect citizens from inadvertent action as well as snooping by the government."

The system is designed to allow the FBI to conduct efficient wiretaps of e-mail conversations and other online communications involving suspected hackers, terrorists and other criminals. The fear among critics is that Carnivore will scoop up transmissions made between innocent civilians and lay them open to scrutiny.

Internet providers, such as Iconn.Net of New Haven, Conn., say Carnivore is unnecessary because they already can do the monitoring the FBI needs if ordered by a court. "We're able to do it faster, more efficiently and, most importantly, without intruding on the privacy of people not within the scope of the search," says Peter William Sachs, president of Iconn.Net, who is scheduled to testify at next week's hearing. EarthLink Inc., one of the nation's largest Internet-service providers, says it refused earlier this year to install Carnivore on its network, claiming technical adjustments required to use the device caused disruptions for its customers.

In its meetings with lawmakers and others, the FBI has described the inner workings of the system in unusual detail. In one demonstration this week, the agency was keen to show how the system could tailor its search so it captures only the e-mails moving into and out of one particular account. The FBI said Carnivore is smart enough to capture a suspect's e-mails while leaving untouched messages sent by his or her spouse or children.

Doc. #10

'Packet Filters'

The system belongs to a class of tools known as "packet filters" or "sniffers," which look for parcels of data that travel across a network and comprise an e-mail or a visit to a Web site. Using a Windows screen, Carnivore also can be set to capture file downloads and chat-room conversations. It can grab e-mail from the most popular Web-based companies, including Yahoo! Inc. and Microsoft Corp.'s Hotmail. And once it is installed at an Internet service provider, the FBI can dial into Carnivore to make changes and monitor data that have been collected.

The FBI is adamant about dispelling fears that Carnivore could be used for rampant tapping of public e-mail systems. For one, wiretapping requests are closely scrutinized by the Justice Department, and must be approved by a federal judge. Abuse by a rogue investigator is even less likely, the bureau says, because the rogue would need too much cooperation from other FBI techies and the Internet service provider, says Marcus Thomas, a developer of the system at Quantico.

Depending on a judge's instructions, Carnivore can be set to merely trace Internet communications to and from a suspect, called a "pen register" or "trap and trace." Carnivore records the Internet addresses of passing traffic but not, for example, the contents or even the subject line of an e-mail. Since the amount of information gathered is relatively small in these instances, even a week's worth of monitoring can be stored on a single floppy disk, the agency says. With judicial permission, the system also can conduct fuller intercepts, which would gather the contents of the e-mails and other data.

The FBI says Carnivore doesn't monitor the content of passing e-mails, a capability widely rumored to exist in the controversial "Echelon" surveillance network operated overseas by the National Security Agency. Bureau officials said watching for key words in passing e-mails was technically possible, but that it would slow Internet traffic unacceptably for all customers. "If you attempt with a machine like this to actually read everything that goes by, you very quickly cannot deal with it," Mr. Thomas says.

The FBI now says it has used Carnivore in fewer than 25 investigations over the past 18 months, most targeting suspected terrorists or computer hackers. In each case, the system was connected to a commercial Internet service provider, where it intercepted data or e-mails in strict compliance with a court order, the FBI says.

Privacy advocates, who haven't been privy to the FBI demonstrations, hunger for much more than explanations. The American Civil Liberties Union wants the FBI to suspend Carnivore's use, arguing that Internet providers can already conduct adequate electronic wiretaps. The ACLU also has filed a request under the Freedom of Information Act for the blueprints of how Carnivore works. Many in the industry want these same plans—called the "source code"—to insure that the system isn't open to abuse and won't disrupt business.

The FBI says making Carnivore's inner workings public would allow hackers to defeat it. "Once you know how it works ... it could be fairly trivial to evade it," Mr. Thomas says.

Legislation to quash Carnivore entirely is unlikely, but lawmakers could move to tighten the requirements for its use or to impose rules that would further protect the privacy of innocent Internet users. Many argue that Carnivore points up the need for Congress to wrestle with a larger dilemma: updating the nation's wiretap laws, hatched long before the Internet existed.

2

From: [redacted] 6C-1/67C-1
To: CHARLES STEELE, DONALD KERR, LARRY PARKINSON, ...
Date: 7/20/00 4:38PM
Subject: DOJ review of statement.

Gentlemen:

Upon giving the "final" draft of Dr. Kerr's statement to OPCA, I was informed that DOJ will also review our final version of the statement before OPCA disseminates it to the Senate.

OPCA anticipates that DOJ will make recommendations to tweak the statement, therefore I'll revise the current FBI approved version with highlighted text of the DOJ recommendations for your review and comments before releasing it back to OPCA.

Dr. Kerr: This note is to confirm that 18 U.S.C. section 2511 does set forth the punishment for intentionally violating both Title III and ECPA.

[redacted] 6C-1
OGC/ILU 67C-1

Doc. #11

From: [redacted]
To:
Date: 7/20/00 6:20PM
Subject: Don Kerr's Testimony

b6-1
b7C-1

b6-1
b7C-1

[redacted]

The revisions that I just gave you do not include a fix for the problem that we just discussed, namely, the difference between T-III's standards for interception of oral/wire communications, and those for electronic communications. The former are set forth in 18 USC 2516(1), the latter in 18 USC 2516(3).

For the purpose of this testimony, the two main differences are:
(1) that applications under 2516(3) do not require senior level DOJ approval and (2) that they are not limited to "certain federal felonies. Thus if we strike the sentence at the bottom of page two/top of page three (referring to authorization by a senior official of DOJ) and the last sentence in the first paragraph of page three ("Further, interception of communications is limited to certain specified felony offenses.") we will remove some of the misleading inferences as to which provision we follow when seeking court approval to intercept e-mail. There may may be other instances where the testimony suggests that we use 2616(1) rather than 2516(3); OGC should scrub the testimony again to check for such instances.

b6-1
b7C-1

[redacted]

CC: [redacted] CHARLES STEELE [redacted]

b6-1
b7C-1

Doc #12

July 21, 2000

URGENT

Note for:

OLC
FBI [redacted] 6C-1 67C-1
OPD
EOUSA
ODAG [redacted] – did you get the FBI's statement from yesterday?) 6C-3 67C-3

From: [redacted] OLA 6C-3 67C-3

Re: CRM statement for 7/24 on "Carnivore" and the 4th amendment

Please provide comments (or "no comment") on the attached by 2 PM today, Friday.

Thanks.

cc: [redacted] OLA
6C-3
67C-3
Please provide c

Doc. #13

STATEMENT OF
KEVIN V. Di GREGORY
DEPUTY ASSISTANT ATTORNEY GENERAL
UNITED STATES DEPARTMENT OF JUSTICE
BEFORE THE SUBCOMMITTEE ON THE CONSTITUTION
OF THE HOUSE COMMITTEE ON THE JUDICIARY
on
"CARNIVORE" AND THE FOURTH AMENDMENT

July 24, 2000

Mr. Chairman and Members of the Subcommittee, thank you for allowing me this opportunity to testify about the law enforcement tool "Carnivore" and the Fourth Amendment. On April 6, 2000, I had the privilege of testifying before you during a hearing on Internet privacy and the Fourth Amendment; I am pleased to continue to participate in the discussion today about "Carnivore" and its role in protecting individual privacy on the Internet from unwarranted governmental intrusion, and about the critical role the Department plays to ensure that the Internet is a safe and secure place.

Privacy and Public Safety

It is beyond dispute that the Fourth Amendment protects the rights of Americans while they work and play on the Internet just as it does in the physical world. The goal is a long-honored and noble one: to preserve our privacy while protecting the safety of our citizens. Our founding fathers recognized that in order for our democratic society to remain safe and our liberty intact, law enforcement must have the ability to investigate, apprehend and prosecute people for criminal conduct. At the same time, however, our founding fathers held in disdain the government's disregard and abuse of privacy in England. The founders of this nation adopted the Fourth Amendment to address the tension that can at times arise between privacy and public

safety. Under the Fourth Amendment, the government must demonstrate probable cause before obtaining a warrant for a search, arrest, or other significant intrusion on privacy.

Congress and the courts have also recognized that lesser intrusions on privacy should be permitted under a less exacting threshold. The Electronic Communications Privacy Act ("ECPA") establishes a three-tier system by which the government can obtain stored information from electronic communication service providers. In general, the government needs a search warrant to obtain the content of unretrieved communications (like e-mail), a court order to obtain transactional records, and a subpoena to obtain information identifying the subscriber. *See* 18 U.S.C. §§ 2701-11.

In addition, in order to obtain source and destination information in real time, the government must obtain a "trap and trace" or "pen register" court order authorizing the recording of such information. *See* 18 U.S.C. 1821 et. Seq.

Because of the privacy values it protects, the wiretap statute, 18 U.S.C. §§ 2510-22, commonly known as Title III, places a higher burden on the real-time interception of oral, wire and electronic communications than the Fourth Amendment requires. In the absence of a statutory exception, the government needs a court order to wiretap communications. To obtain such an order, the government must show that normal investigative techniques for obtaining the information have or are likely to fail or are too dangerous, and that any interception will be conducted so as to ensure that the intrusion is minimized.

The safeguards for privacy represented by the Fourth Amendment and statutory restrictions on government access to information do not prevent effective law enforcement. Instead, they provide boundaries for law enforcement, clarifying what is acceptable evidence

gathering and what is not. At the same time, those who care deeply about protecting individual privacy must also acknowledge that law enforcement has a critical role to play in preserving privacy. When law enforcement investigates, successfully apprehends and prosecutes a criminal who has stolen a citizen's personal information from a computer system, for example, law enforcement is undeniably working to protect privacy and deter further privacy violations. The same is true when law enforcement apprehends a hacker who compromised the financial records of a bank customer.

As we move into the 21st century, we must ensure that the needs of privacy and public safety remain in balance and are appropriately reflected in the new and emerging technologies that are changing the face of communications. Although the primary mission of the Department of Justice is law enforcement, Attorney General Reno and the entire Department understand and share the legitimate concerns of all Americans with regard to personal privacy. The Department has been and will remain committed to protecting the privacy rights of individuals. We look forward to working with Congress and other concerned individuals to address these important matters in the months ahead.

Law Enforcement Tools in Cyberspace:

Although the Fourth Amendment is over two centuries old, the Internet as we know it is still in its infancy. The huge advances in the past ten years have changed forever the landscape of society, not just in America, but worldwide. The Internet has resulted in new and exciting ways for people to communicate, transfer information, engage in commerce, and expand their educational opportunities. These are but a few of the wonderful benefits of this rapidly changing technology. As has been the case with every major technological advance in our history,

however, we are seeing individuals and groups use this technology to commit criminal acts. As Deputy Attorney General Eric Holder told the Crime Subcommittee of this Committee in February, our vulnerability to computer crime is astonishingly high and threatens not only our financial well-being and our privacy, but also this nation's critical infrastructure.

Many of the crimes that we confront everyday in the physical world are beginning to appear in the online world. Crimes like threats, extortion, fraud, identity theft, and child pornography are migrating to the Internet. The Fourth Amendment and laws addressing privacy and public safety serve as a framework for law enforcement to respond to this new forum for criminal activity. If law enforcement fails properly to respect individual privacy in its investigative techniques, the public's confidence in government will be eroded, evidence will be suppressed, and criminals will elude successful prosecution. If law enforcement is too timid in responding to cybercrime, however, we will, in effect, render cyberspace a safe haven for criminals and terrorists to communicate and carry out crime, without fear of authorized government surveillance. If we fail to make the Internet safe, people's confidence in using the Internet and e-commerce will decline, endangering the very benefits brought by the Information Age. Proper balance is the key.

To satisfy our obligations to the public to enforce the laws and preserve the safety, we use the same sorts of investigatory techniques and methods online as we do in the physical world, with the same careful attention to the strict constitutional, statutory, internal and court-ordered boundaries. Carnivore is simply an investigatory tool that is used online only under narrowly defined circumstances, and only when authorized by law, to meet our responsibilities to the public.

To illustrate, law enforcement often needs to find out from whom a drug dealer, for instance, is buying his illegal products, or to whom the drug dealer is selling. To investigate this, it is helpful to determine who is communicating with the drug dealer. In the "olden days" of perhaps 10 years ago, the drug dealer would have communicated with his supplier and customers exclusively through use of telephones and pagers. Law enforcement would obtain an order from a court authorizing the installation of a "trap and trace" and a "pen register" device on the drug dealer's phone or pager, and either the telephone company or law enforcement would have installed these devices to comply with the court's order. Thereafter, the source and destination of his phone calls would have been recorded. This is information that courts have held is not protected by any reasonable expectation of privacy. Given the personal nature of this information, however, the law requires government to obtain an order under these circumstances. In this way, privacy is protected and law enforcement is able to investigate to protect the public.

Now, that same drug dealer may be just as likely to send an e-mail as call his confederates. When law enforcement uses a "trap and trace" or "pen register" in the online context, however, we have found that, at times, the Internet service provider has been unable or even unwilling to supply this information. Law enforcement cannot abdicate its responsibility to protect public safety simply because technology has changed. Rather, the public rightfully expects that law enforcement will continue to be effective as criminal activity migrates to the Internet. We cannot do this without tools like Carnivore.

When a criminal uses e-mail to send a kidnaping demand, to buy and sell illegal drugs or to distribute child pornography, law enforcement needs to know to whom he is sending messages and from whom he receives them. To get this information, we obtain a court order, which we

serve on the appropriate service provider. Because of the nature of Internet communications, the addressing information (which does not include the content of the message) is often mixed in with a lot of other non-content data that we have no desire or authority to gather. If the service provider can comply with the order and provide us with only the addressing information required by court order, it will do so and we will not employ Carnivore. If, however, the service provider is unwilling or unable to comply with the order, we simply cannot give a criminal a free pass. It is for that narrow set of circumstances that the FBI designed "Carnivore."

Carnivore is, in essence, a special filtering tool that can gather the information authorized by court order, and only that information. It permits law enforcement, for example, to gather only the email addresses of those persons with whom the drug dealer is communicating, without allowing any human being, either from law enforcement or the service provider, to view private information outside of the scope of the court's order. In other words, Carnivore is a *minimization* tool that permits law enforcement strictly to comply with court orders, strongly to protect privacy, and effectively to enforce the law to protect the public interest. In addition, Carnivore creates an audit trail that demonstrates exactly what it is capturing.

As with any other investigative tools, there are many mechanisms we have in place to prevent against possible misuse of Carnivore, and to remedy misuse that has occurred. The Fourth Amendment, of course, restricts what law enforcement can do with Carnivore, as do the statutory requirements of Title III and the Electronic Communications Privacy Act, and the courts.

For federal Title III applications, the Department of Justice imposes its own guidelines on top of the privacy protections provided by the Constitution, statutes and the courts. For example,

before Carnivore may be used to intercept wire or electronic communications, the requesting investigatory agency must obtain approval from the Department of Justice. Specifically, the Office of Enforcement Operations in the Criminal Division of the Department reviews each proposed Title III application to ensure that the interception satisfies the Fourth Amendment requirements, and is in compliance with applicable statutes and regulations. Similarly, typically the U.S. Attorney or the section chief within the Department who is handling the investigation also reviews the Title III intercept request. Even if the proposal clears the OEO, approval must be given by a Deputy Assistant Attorney General. Although this requirement of high-level review is required by Title III only with regard to proposed intercepts of wire and oral communications, the Department voluntarily imposes the same level of review for proposed interceptions of electronic communications (except digital-display pagers). Typically, investigative agencies such as the Federal Bureau of Investigation have similar internal requirements, separate and apart from Constitutional, statutory or Department of Justice requirements.

If the investigative agency and the Department of Justice approve a federal Title III request, it still must, of course, be approved by the proper court. The court will evaluate the application under the Fourth Amendment and using the familiar standards of Title III. By statute, for example, the application to the court must show, through sworn affidavit, why the intercept is necessary as opposed to other less-intrusive investigatory techniques. The application must also provide additional detail, including whether there have been previous interceptions of communications of the target, the identity of the target (if known), the nature and location of the communications facilities, and a description of the type of communications sought and the

offenses to which the communications relate. By statute and internal Department regulation, the interception may last no longer than 30 days without an extension by the court.

Courts also often impose their own requirements. For example, many federal courts require that the investigators provide periodic reports setting forth information such as the number of communications intercepted, steps taken to minimize irrelevant traffic, and whether the interceptions have been fruitful. The court may, of course terminate the interception at any time.

The remedies for violating Title III or ECPA by improperly intercepting electronic communications can include criminal sanctions, civil suit, and for law enforcement agents, adverse employment action. For violations of the Fourth Amendment, of course, the remedy of suppression is also available.

Carnivore itself also contains self-regulating features. For example, because of its sophisticated passive filtering features, it automates the process of minimization without intrusive monitoring by investigators, and simply disregards packets of information that do not satisfy the criteria in the court's authorization. Indeed, one of the most powerful privacy-protecting features of Carnivore is its ability to ignore information that is outside the scope of the court-ordered authority. For later verification, it also logs the filter settings. In addition, as a practical matter, Carnivore is not deployed except with close cooperation with the appropriate system provider. In any event, the FBI does not use Carnivore in every instance in which the court orders a Title III electronic communication intercept. Indeed, I understand that the Bureau uses Carnivore only in those instances when the service provider is unable to comply with the court order using its own equipment, or when the provider asks the FBI to use Bureau equipment.

As I testified in April, we face three major categories of challenges in trying to keep the Internet a safe and secure place for our citizens. These are:

1. Technical challenges that hamper law enforcement's ability to locate and prosecute criminals that operate online;
2. Certain substantive and procedural laws that have not kept pace with the changing technology, creating significant legal challenges to effective investigation and prosecution of crime in cyberspace; and
3. Resource needs that must be addressed to ensure that law enforcement can keep pace with changing technology and has the ability to hire and train people to fight cybercrime.

Carnivore is an investigative tool that assists us in meeting the first challenge. As we have witnessed, tracking a criminal online is not always an impossible task using our investigative tools. For example, last year federal and state law enforcement combined to successfully apprehend the creator of the Melissa virus and the individual who created a fraudulent Bloomberg News Service website in order to artificially drive up the stock price of PairGain, a telecommunications company based in California. Although we are proud of these important successes, we still face significant challenges as online criminals become more and more sophisticated.

In nearly every online case, tracking the online criminal requires law enforcement to attempt to trace the "electronic trail" from the victim back to the perpetrator. In effect, this "electronic trail" is the fingerprint of the twenty-first century – only much harder to find and not

as permanent as its more traditional predecessor. In the physical world, a criminal and his victim are generally in the same location. But cybercriminals do not have to physically visit the crime scene. Instead they cloak their illegal activity by weaving communications through a series of anonymous remailers, by creating forged e-mail headers with powerful point and click tools readily downloadable from hacker websites, by using a "free-trial" account or two, or by "wiping clean" the logging records that would be evidence of their activity.

In some cases, the criminal may not even be in the same country as the victim. The global nature of the Internet, while one of the greatest assets of the Internet to law-abiding citizens, allows criminals to conduct their illegal activity from across the globe. In these cases, the need to respond quickly and track the criminal is increasingly complicated and often frustrated by the fact that the activity takes place throughout different countries. With more than 190 countries connected to the Internet, it is easy to understand the coordination challenges that face law enforcement. Furthermore, in these cases, time is of the essence and the victim may not even realize they have been victimized until the criminal has long since signed-off. Clearly, the technical challenges for law enforcement are real and profound.

This fact was made clear in the findings and conclusions reached in the recently released report of the President's Working Group on Unlawful Conduct on the Internet, entitled, "The Electronic Frontier: The Challenge of Unlawful Conduct Involving the Use of the Internet." This extensive report highlights in detail the significant challenges facing law enforcement in cyberspace. As the report states, the needs and challenges confronting law enforcement, "are neither trivial nor theoretical." The Report outlines a three-pronged approach for responding to unlawful activity on the Internet:

1. Conduct on the Internet should be treated in the same manner as similar conduct offline, in a technology neutral manner.
2. We must recognize that the needs and challenges of law enforcement posed by the Internet are substantial, including our the need for resources, up-to date investigative tools and enhanced multi-jurisdictional cooperation.
3. Finally, continued support for private sector leadership in developing tools and methods to help Internet users to prevent and minimize the risks of unlawful conduct online.

I would encourage anyone with an interest in this important topic to review carefully the report of the Working Group. The report can be found on the Internet by visiting the website of the Department of Justice's Computer Crime and Intellectual Property Section, located at www.cybercrime.gov. In addition to the report, www.cybercrime.gov also contains other useful information on a wide array of Internet related issues, including the topic of today's hearing – privacy.

Despite the type of difficulties outlined in the Unlawful Conduct Report and discussed today, the Justice Department and law enforcement across this nation are committed to continuing to work together and with their counterparts in other countries to develop and implement investigative strategies to successfully track, apprehend, and prosecute individuals who conduct criminal activity on the Internet. In so doing, the same privacy standards that apply in the physical world remain effective online.

Mr. Chairman, the Department of Justice has taken a proactive leadership role in making cyberspace safer for all Americans. The cornerstone of our cybercrime prosecutor program is the

Criminal Division's Computer Crime and Intellectual Property Section, known as CCIPS. CCIPS was founded in 1991 as the Computer Crime Unit, and became a Section in 1996. CCIPS has grown from five attorneys in 1996 to twenty today – and we need more to keep pace with the demand for their expertise. The attorneys in CCIPS work closely on computer crime cases with Assistant United States Attorneys known as "Computer and Telecommunications Coordinators," or CTC's, in U.S. Attorney's Offices around the nation. Each CTC receives special training and equipment and serves as the district's expert on computer crime cases. CCIPS and the CTC's work together in prosecuting cases, spearheading training for local, state and federal law enforcement, working with international counterparts to address difficult international challenges, and providing legal and technical instruction to assist in the protection of this nation's critical infrastructures. We are very proud of the work these people do and we will continue to work diligently to help stop criminals from victimizing people online.

I also note that public education is an important component of the Attorney General's strategy on combating computer crime. As she often notes, the same children who recognize that it is wrong to steal a neighbor's mail or shoplift do not seem to understand that it is equally wrong to steal a neighbor's e-mail or copy a proprietary software or music file without paying for it. To remedy this problem, the Department of Justice, together with the Information Technology Association of America (ITAA), has embarked upon a national campaign to educate and raise awareness of computer responsibility and to provide resources to empower concerned citizens. The "Cybercitizen Awareness Program" seeks to engage children, young adults, and others on the basics of critical information protection and security and on the limits of acceptable online behavior. The objectives of the program are to give children an understanding of cyberspace

benefits and responsibilities, an awareness of consequences resulting from the misuse of the medium and an understanding of the personal dangers that exist on the Internet and techniques to avoid being harmed.

Conclusion:

Mr. Chairman, I want to thank you again for this opportunity to testify today about our efforts to fight crime on the Internet while preserving the rights conferred by the Fourth Amendment and statute. Ultimately, the decision as to the appropriate parameters of law enforcement activity lies squarely within the Constitution and the elected representatives of the people, the Congress. The need to protect the privacy of the American people -- not just from the government but also from criminals -- is a paramount consideration, not just in the context of the Internet, but in general. The Department of Justice stands ready to work with this Subcommittee and others to achieve the proper balance between the important need for protecting privacy and the need to respond to the growing threat of crime in cyberspace.

Mr. Chairman, that concludes my prepared statement. I would be pleased to attempt to answer any questions that you may have at this time.

-original (since finished)

Statement for the Record of
Donald M. Kerr
Assistant Director
Federal Bureau of Investigation
Before the
United States House of Representatives
The Committee on the Judiciary
Subcommittee on the Constitution
Washington, D.C.
7/24/2000

Good afternoon, Mr. Chairman, and Members of the Subcommittee. I am grateful for this opportunity to discuss the FBI's Internet and data interception capabilities and to help set the record straight regarding this important issue. I would like to first discuss FBI's legal authority for conducting interceptions on the Internet, and then describe Carnivore and how we use it.

Two weeks ago, the Wall Street Journal published an article entitled "FBI's system to covertly search e-mail raises privacy, legal issues." This story was immediately followed by a number of similar reports in the press and other media depicting Carnivore as something ominous and raising concerns about the possibility of its potential to snoop, without a court order, into the private E-mails of American citizens. I think that it is important that this topic be discussed openly--and in fact this was the purpose behind the FBI choosing to share information regarding this capability with the industry experts several weeks ago. It is critically important that, as technology, and particularly communications technology, continues to evolve rapidly, the public be guaranteed that their government is observing the statutory and constitutional protections which they demand. I believe that it is also very important that these discussions be placed into the context into which they properly belong and that the true facts concerning this issue are made clear. More to the point,

that these capabilities are used only with lawful authorization and that they are directed at the most egregious violations of national security and public safety.

First of all, the FBI performs interceptions of criminal wire and electronic communications, including Internet communications, under authorities derived in part from Title III of the Omnibus Crime Control and Safe Streets Act of 1968 (as amended), which is commonly referred to as "Title III", and portions of the Electronic Communications Privacy Act of 1986 (as amended), or "ECPA". I want to stress that all such interceptions, with the exception of a rarely used "emergency" authority or consent of a participant in the communication, are performed under a court order issued by a judge. Under emergency provisions, the Attorney General, the Deputy or the Associate Attorney General may, if authorized, initiate electronic surveillance of wire or electronic communications without a court order, but only if an application for such order is made within 48 hours after the surveillance is initiated.

Federal surveillance laws must comply with the Fourth Amendment's dictates concerning reasonable searches and seizures, but they also include a number of provisions that are intended to ensure that this investigative technique is used judiciously and with deference to the privacy of intercepted subjects and certainly with deference to the privacy of those who are not the subject of the court order.

For example, unlike search warrants for physically searching a house, under Title III and Department of Justice policy, applications for interception of oral, wire and electronic

communications require the authorization of a high-level Department of Justice (DOJ) official before the local United States Attorneys offices can make an application to a federal court. Further, interception of communications is limited to certain federal criminal offenses.

Applications for electronic surveillance must demonstrate probable cause and state with particularity and specificity: the offenses being committed, the telecommunications facility or place from which the subject's communications are to be intercepted, a description of the types of conversations to be intercepted, and the identities of the persons committing the offenses and anticipated to be intercepted. Thus, criminal electronic surveillance laws focus on gathering hard evidence-- not intelligence.

Applications must indicate that other normal investigative techniques have been tried and failed to gather evidence of crime, or will not work, or are too dangerous, and must include information concerning any prior electronic surveillance regarding the subject or facility in question. Court orders are initially limited to 30 days, with extensions possible, and must terminate sooner if the objectives are obtained. Judges may, and usually do, require periodic reports to the court, typically every 7 to 10 days, advising it of the progress of the interception effort. This assures close and on-going oversight of the electronic surveillance by the United States Attorney's office handling the case and frequently the court.

Interceptions are required to be conducted in such a way as to "minimize the interception of communications not otherwise subject to interception" under the law, such as unrelated, irrelevant, and non-criminal communications of the subjects and of others not named in the application.

To ensure privacy protection and evidentiary integrity of the communications that are intercepted, such intercepted communications are required to be recorded, if possible, on tape or other device, and recorded in such a way as will protect the recording from editing or other alterations. Immediately upon the expiration of the interception period, these recordings are then required to be presented to the federal district court judge and sealed under his or her directions. The presence of the seal shall be a prerequisite for their use or disclosure, or for the introduction of evidence derived from the tapes. Applications and orders signed by the judge are also to be sealed by the judge.

Within a reasonable period of time after the termination of the intercept order, including extensions, the judge shall ensure that the subject of the interception order, and other parties as are deemed appropriate, are furnished an inventory, providing notice of the order, the dates during which the interceptions were carried out, and whether or not the person was intercepted. Upon motion, the judge may also direct that portions of the contents of the intercepted communication be made available to for their inspection.

Any person who was a party to an intercepted communication or was a party against whom an interception was directed may in any trial, hearing, or other proceeding move to suppress the con-

tents of any intercepted communication or any evidence derived therefrom if there are grounds demonstrating that the communication was intercepted in violation of Title III, ECPA or the Fourth Amendment.

The illegal, unauthorized conduct of electronic surveillance is a federal criminal offense punishable by imprisonment for up to five years, a fine, or both. In addition, any person whose communications are unlawfully intercepted, disclosed, or used, may in a civil action recover from the person or entity engaged in the violation civil damages, including, if appropriate, punitive damages, as well as attorney's fees and other costs incurred.

The technical assistance of the service providers in helping a law enforcement agency execute an electronic surveillance order is always important, and in many cases it is absolutely essential. This circumstance is increasingly the case with the advent of advanced communications services and networks such as the Internet. Title III mandates service provider assistance incidental to law enforcement's execution of electronic surveillance orders by specifying that a court order authorizing the interception of communications shall upon the request of the applicant, direct that a "service provider, landlord, custodian, or other person shall furnish the applicant forthwith all information, facilities, and technical assistance necessary to accomplish the interception unobtrusively and with a minimum of interference with the services that such service provider, landlord, custodian, or person is according the person whose communications are to be intercepted."

In practice, judges may sign two orders: one order authorizing the law enforcement agency to conduct the electronic surveillance, and a second, abbreviated, assistance order directed to the service provider, specifying, for example in the case of E-mail, the E-mail account name of the subject that is the object of the order and directing the provision of necessary assistance.

Service providers and their personnel are subject to the electronic surveillance laws like public officials and private persons. That is, unauthorized electronic surveillance is forbidden, and criminal and civil liability may be assessed for violations. Not only are unauthorized interceptions proscribed, but so also is the use or disclosure of the contents of communications that have been illegally intercepted. It is for this reason, among others, that service providers typically take great care in providing assistance to law enforcement in carrying out electronic surveillance pursuant to court order. In some instances, service providers opt to provide "full" service, essentially carrying out the interception for law enforcement and providing the final interception product, but, in most cases, service providers are inclined only to provide the level of assistance necessary to allow the law enforcement agency to conduct the interception. I want to stress that the FBI does not conduct interceptions, install and operate pen registers, or use trap & trace devices without lawful authorization from a court.

In recent years, it has become increasingly common for the FBI to seek, and for judges to issue, orders for Title III interceptions which are much more detailed than older orders which were directed against "plain old telephone services." These detailed orders, in order to be successfully implemented, require complex approaches to ensure that only messages for which there is

probable cause to intercept are, in fact, intercepted. The fact that court orders are becoming more detailed is in response, I think, to two facts.

First, the complexity of modern communications networks, like the Internet, as well as the complexity of modern users' communications demand better discrimination than for older analog communications. For example, Internet users frequently use electronic messaging services, like E-mail, to communicate with other individuals in a manner reminiscent of a telephone call, only with text instead of voice. Such messages are often the targets of court ordered interception. Users also use services, like the world wide web, which looks more like print media than a phone call. Similarly, some Internet services, like streaming video, have more in common with broadcast media like television, than with telephone calls. These types of communications are less commonly the targets of an interception order.

The second fact is that for many Internet services, users share communications channels, addresses, etc. These facts make the interception of messages for which law enforcement has probable cause, to the exclusion of all others, very difficult. Court orders are therefore increasingly written to include detailed instructions for ensuring that the privacy of communications for which there is no probable cause to intercept is guaranteed.

In response to a critical need for tools to implement these complex court orders, the FBI developed a number of capabilities including the software program called "Carnivore." Carnivore is a very specialized network analyzer or "sniffer" which runs on a normal Personal Computer running the

Microsoft Windows operating system. It works by "sniffing" the proper portions of network packets and copying and storing only those packets which match a finely defined filter set programed in conformity with the court order. This filter set can be extremely complex, and this provides the FBI with an ability to collect transmissions which comply with pen register court orders, trap & trace court orders, Title III interception orders, etc.

It is important to distinguish now what is meant by "sniffing." The problem of discriminating between users' messages on the Internet is a complex one. However, this is exactly what Carnivore does. It does NOT search through the contents of every message and collect those that contain certain key words like "bomb" or "drugs." It selects messages based on criteria expressly set out in the court order, for example, messages transmitted to or from a particular account or to or from a particular user. If the device is placed at some point on the network where it cannot discriminate messages as set out in the court order, it simply lets all such messages pass by unrecorded.

One might ask, "why use Carnivore at all?" In many instances, ISPs, particularly the larger ones, maintain capabilities which allow them to comply, or partially comply with lawful orders. For example, many ISPs have the capability to "clone" or intercept, when lawfully ordered to do so, E-mail to and from specified user accounts. In such cases, these abilities are satisfactory and allow full compliance with a court order. However, in most cases, ISPs do not have such capabilities or cannot employ them in a secure manner. Also, most systems devised by service providers or purchased "off the shelf" lack the ability to properly discriminate between messages in a fashion

that complies with the court order. Also, many court orders go beyond E-mail, specifying other protocols to be intercepted such as instant messaging. In these cases, a cloned mailbox is not sufficient to comply with the order of the court.

Now, I think it is important that you understand how Carnivore is used in practice. First, there is the issue of scale. Carnivore is a small-scale device intended for use only when and where it is needed. In fact, each Carnivore device is maintained at the FBI Laboratory in Quantico until it is actually needed in an active case. It is then deployed to satisfy the needs of a single case or court order, and afterwards, upon expiration of the order, the device is removed and returned to Quantico.

The second issue is one of network interference. Carnivore is safe to operate on IP networks. It is connected by a high impedance bridge and does not have any ability to transmit anything onto the network. In fact, we go to great lengths to ensure that the Carnivore is satisfactorily isolated from the network to which it is attached. Also, Carnivore is only attached to the network after consultation with, and with the agreement of, technical personnel from the ISP.

This, in fact raises the third issue--that of ISP cooperation. To date, Carnivore has, to my knowledge, never been installed onto an ISP's network without assistance from the ISP's technical personnel. The Internet is a highly complex and heterogeneous environment in which to conduct such operations, and I can assure you that without the technical knowledge of the ISP's personnel, it would be very difficult, and in some instances impossible, for law enforcement agencies to

successfully implement, and comply with the strict language, of an interception order. The FBI also depends upon the ISP personnel to understand the protocols and architecture of their particular networks.

Another primary consideration for using Carnivore is data integrity. As you know, Rule 901 of the Federal Rules of Evidence require the authentication of evidence as a precondition for its admissibility. The use of the Carnivore system by the FBI to intercept and store communications provides for an undisturbed chain of custody by providing a witness who can testify to the retrieval of the evidence and the process by which it was recorded. Performance is also a key reason for the use of Carnivore over commercial sniffers. Unlike commercial software sniffers, Carnivore is designed to intercept and record the selected communications comprehensively, without "dropped packets."

In conclusion, I would like to say that over the last five years or more, we have witnessed a continuing, steady growth in instances of computer-related crimes, including traditional crimes and terrorist activities which have been planned or carried out, in part, using the Internet. The ability of the law enforcement community to effectively investigate and prevent these crimes is, in part, dependant upon our ability to lawfully collect vital evidence of wrongdoing. As the Internet becomes more complex, so do the challenges placed on us to keep pace. We could not do so without the continued cooperation of our industry partners and innovations such as the Carnivore software.

I look forward to working with the subcommittee staff to provide more information and welcome your suggestions on this important issue. I will be happy to answer any questions that you may have. Thank You.

View Related Topics

July 24, 2000, Monday

TYPE: COMMITTEE HEARING

LENGTH: 33615 words

HEADLINE: U.S. REPRESENTATIVE CHARLES CANADY (R-FL) HOLDS HEARING REGARDING THE **CARNIVORE** SYSTEM; WASHINGTON, D.C.

BODY:
HOUSE COMMITTEE ON THE JUDICIARY SUBCOMMITTEE ON THE

CONSTITUTION HOLDS HEARING REGARDING THE **CARNIVORE**

SYSTEM

JULY 24, 2000

SPEAKERS: U.S. REPRESENTATIVE CHARLES T. CANADY (R-FL), CHAIRMAN

U.S. REPRESENTATIVE HENRY J. HYDE (R-IL)

U.S. REPRESENTATIVE ASA HUTCHINSON (R-AR)

U.S. REPRESENTATIVE SPENCER BACHUS (R-AL)

U.S. REPRESENTATIVE BOB GOODLATTE (R-VA)

U.S. REPRESENTATIVE BOB BARR (R-GA)

U.S. REPRESENTATIVE WILLIAM L. JENKINS (R-TN)

U.S. REPRESENTATIVE LINDSEY GRAHAM (R-SC)

U.S. REPRESENTATIVE MELVIN L. WATT (D-NC)

RANKING MEMBER

U.S. REPRESENTATIVE MAXINE WATERS (D-CA)

U.S. REPRESENTATIVE BARNEY FRANK (D-MA)

U.S. REPRESENTATIVE JOHN CONYERS (D-MI)

U.S. REPRESENTATIVE JERROLD NADLER (D-NY)

KEVIN DIGREGORY, DEPUTY ASSOCIATE ATTORNEY GENERAL

Doc #14

DAVID GREEN, DEPUTY CHIEF

COMPUTER CRIME AND INTELLECTUAL PROPERTY SECTION

DEPARTMENT OF JUSTICE'

DONALD KERR, DIRECTOR

LAB DIVISION

FEDERAL BUREAU OF INVESTIGATION

LARRY PARKINSON, GENERAL COUNSEL

FEDERAL BUREAU OF INVESTIGATION

ALAN DAVIDSON, STAFF COUNSEL

CENTER FOR DEMOCRACY AND TECHNOLOGY

MATT BLAZE, RESEARCH SCIENTIST

AT&T LABS

BARRY STEINHARDT, ASSOCIATE DIRECTOR

AMERICAN CIVIL LIBERTIES UNION

ROBERT CORN-REVERE

HOGAN AND HARTSON

STEWART BAKER

STEPTOE AND JOHNSON

PETER SACHS

ICONN, LLC

TOM PERRINE, MANAGER OF SECURITY TECHNOLOGIES

SAN DIEGO SUPER COMPUTER CENTER

*** Elapsed Time 00:00, Eastern Time 13:04 ***

*

CANADY: The subcommittee will be in order. And it's probably going to be necessary for the staff to close the doors, otherwise we'll have noise from the hallways.

In recent years, with the growth of the Internet, the **FBI** has encountered an increasing number of criminal investigations in which criminal subjects have used the Internet to communicate with each other or their victims.

Because the **FBI** believes many Internet service providers lack the ability to discriminate between communications in order to isolate the specific types of information that may be authorized to be gathered under a court order, the **FBI** has designed and developed a program called **Carnivore** which enables the **FBI** to isolate, intercept and collect communications that are the subject of lawful orders.

The first news of **Carnivore** came in April during testimony before the Subcommittee on the Constitution by attorney Robert Corn-Revere, who represented an Internet service provider that tried to resist attaching the **Carnivore** program to its network.

It has also been reported that one of the nations largest Internet service providers, EarthLink, Inc., has refused to install **Carnivore** on its network because attaching the program in the past caused its remote access servers to crash, eliminating service to customers.

Other ISPs have stated publicly that they would challenge an order to attach to their networks.

While these industry officials have expressed willingness to cooperate with law enforcement to comply with legitimate court orders, they're concerned about the effects attaching **Carnivore** to their networks will have on the security of their infrastructure and the privacy of their customers.

At a press conference on July 12, Attorney General Reno stated that she does not want **Carnivore**, quote, "to be a tool that is in any way a cause of concern for privacy interests," close quote. Today's hearing provides federal law enforcement the opportunity to address the privacy concerns that have been raised.

More broadly, **Carnivore** raises the question as to whether existing statutes protecting citizens from unreasonable searches and seizures under the Fourth Amendment appropriately balance the concern of law enforcement and privacy. Law enforcement is concerned that the information needed to keep the public safe remains available. Individual citizens are concerned that a sufficient degree of privacy and the integrity of personal information be maintained in an age of modern communications and information storage where information that may have traditionally been kept in a file cabinet at home is now electronically stored by a third party in cyberspace. The hearing today will also address this balance of interests.

As we consider the use of **Carnivore**, it is important that our deliberations be based on facts and not on unsupported suspicions and irrational fears. At the same time, we should be sensitive to any potential for abuse of the **Carnivore** system. Even a system designed with the best of intentions -- to legally carry out essential law enforcement functions -- may be a cause for concern if its use is not properly monitored.

I look forward to hearing from all of our witnesses today and I'd now recognize Mr. Watt.

WATT: Thank you, Mr. Chairman.

I confess that up until about 10 days to two weeks ago, I had paid very little attention to this whole **Carnivore** project. And at about that point I started to get inquiring telephone calls from the media and press about what I knew about **Carnivore.** I don't know much more about it today, and that's why I want to start by praising the chair of the subcommittee for convening this hearing, because I agree with the chair that whatever information we have and however we proceed as a committee and as a Congress needs to be based on the facts.

So I try to bring to this hearing a level of open-mindedness to try to understand the facts and try to figure out with as much of an open mind as I can what disposition, if any, may be required by Congress, what legislative steps may be warranted.

I suppose I would be less than honest if I didn't say that I have had for quite a while a generalized concern about the government's ability to invade the privacy of its citizens. There seems to me to be a growing level of generalized concern about Big Brotherism that I suspect is being fed by the increasing electronic world.

WATT: When the Fourth Amendment was passed and put into the Constitution, there was at least a feeling that if the government came to do a search, it at least had to bring a warrant and present it to you or come and kick-in your door.

And in some of our communities, we have always had probably an exaggerated fear of whether the latter was likely to occur than the former, and it's probably from that perspective that I have always had this kind of generalized concern.

But notwithstanding that, I will make every effort I can to try to be objective and impartial about this issue. And I think those general comments point up the context in which we're operating and point up the importance of having such a hearing as this.

From my perspective it's good to see a number of people, who as long as the unwarranted searches and wiretaps and invasions or potential invasions were being visited on parts of the community that they weren't necessarily that interested in protecting any way -- it's great to see some greater exposure and concern being expressed about what our government does and how it does it. And this gives us an opportunity to look into that and evaluate it. And I welcome the opportunity and thank the chairman for convening the hearing for that purpose.

Thank you, Mr. Chairman. I yield back.

CANADY: Thank you, Mr. Watt.

Mr. Hyde?

HYDE: Thank you, Mr. Chairman.

Very briefly, this is a very important hearing, as attested to by the interest shown with so many people here today. But the tension between the law enforcement forces of our country, symbolized and personified by the **Federal Bureau of Investigation**, who need access to information if they are to stay on top of terrorists, counterfeiters, drug dealers, criminals of all sorts, the need for that information comes into tension with the need for the public -- for average citizens to have privacy, which is a very valued commodity. So that tension creates serious problems that it is the job of legislators to try to and solve. And that's what we're going to try and do in this hearing and succeeding hearings.

So I congratulate, you, Mr. Canady, for calling this hearing, and I welcome the statements of our friends, the witnesses from the **FBI** and others, and will follow this with great interest. Nothing could be more important in terms of national security and in protecting constitutional rights. I hope we get a good solution.

Thank you, Mr. Chairman.

CANADY: Thank you, Mr. Chairman.

Mr. Conyers?

CONYERS: Thank you very much.

Over the past few weeks, the details about this I hope misnamed technology has begun to emerge. We all know that it was only a matter of time before law enforcement would develop ability to conduct the equivalent of wiretaps on the Internet.

CONYERS: The news about **Carnivore** comes at a time when there is growing concern about how many Americans sacrifice their privacy by using it. Not only do web sites get all kinds of information about us when we make purchases online, or even when we just surf the web, but now we learn that the **FBI** can read our e-mails in the course of a criminal investigation.

So where I come from in the beginning on this is that, are we minimizing the interception of non-incriminating communications of a target of a wiretap order or are we maximizing the law enforcement access to the communication of non-targets? And I think this is a very important question that has to be resolved.

It's not at all clear that the law enforcement should use authority under pen-registers, to the pen-register statute, to access a variety of data. And it's not clear that law enforcement can install a super-trap to get the information that they think that they need.

Now, the Internet, as it takes its place along side the telephone and snail mail as a central means of communication, illegal activities are migrating there as well. And within constitutional boundaries, law enforcement tools -- law enforcement needs tools to be able to intercept unlawful communications by those who will use the Internet for illegal conduct in the hope that they can conspire without leaving fingerprints or footprints.

CONYERS: And at the same time, **Carnivore** -- I said I wasn't going to say that word -- at the same time, this system that we're looking at today mustn't bite off more than it can chew when it comes to **FBI's** electronic surveillance activities. Constitutional rights don't end where cyberspace begins.

And in many ways, today's hearing is not a new story. The potential for law enforcement to overstep constitutional boundaries for electronic surveillance on a new stage goes way back to the 1970s when the Church committee investigated the **FBI's** use of electronic surveillance against Dr. Martin Luther King Jr. The committee then recognized that technological developments in this century have rendered that most private conversations of Americans are vulnerable to interception and monitoring by government agents. So now in this new century, the Church committee's conclusion is timely -- is as timely as ever.

So should we now be comfortable with a "trust us, we're the government" approach? I don't think anybody on the committee has this view.

And I hope the hearing marks the beginnings of a careful examination of how the **FBI's** technology fits within the existing laws and the new technology. And I hope that this hearing will put to rest our fears about this system. Maybe they're unfounded. Maybe it's unclear and we'll need some legislative guidance for our law enforcement.

Does it give the **FBI** the ability to conduct indiscriminate searches of an individual's e-mail activity beyond what a court order would allow? Does it give the **FBI** the ability to search more than is permitted under the agency's pen-register and trap-and-trace authority? And why does the **FBI** need to put this system's terminals on-site at Internet service providers rather than letting the ISP turn over the information that the **FBI** needs, much in the same way the telephone company itself does.

These are the questions I'm looking forward to having some resolution -- and I'm happy that we're here inquiring into this matter.

I ask that the statement of another member, Congresswoman Zoe Lofgren, be included in these opening remarks.

CANADY: Without objection, it will be included in the record.

CONYERS: Thank you.

CANADY: The gentleman from Arkansas is now recognized for five minutes.

HUTCHINSON: Thank you, Mr. Chairman. And I, likewise, express my appreciation for your leadership on scheduling this hearing.

I want to just make a couple of brief comments. First of all, I want to extend my appreciation to the **FBI** and the Department of Justice for the way they have been open about this new technology.

HUTCHINSON: It's my understanding that you have allowed the media to review it; you have provided

demonstrations of this. And I think this is exactly the type of approach that we need to have when we're looking into a new arena of your legitimate needs for surveillance of suspects.

And I think the more the public knows, the more the Congress knows, and the more light that is shed, then the better judgments that will be rendered. And so, I do believe that the **FBI** has engaged in this **Carnivore** as a minimization tool, to limit the review of third- party documents as well -- or content -- as well as that of the suspect's.

But I think that there are some legitimate questions that need to be asked. One, is this new technique properly monitored? We're entering again into an arena that I did not have when I was a United States attorney back in the '80s. We had Title IIIs, we had court approval, we had pen registers, but this is a totally new environment. And I think that the **FBI** has to step gingerly, but we all, obviously, have a responsibility to engage in legitimate law enforcement activities in terms of surveillance.

But who monitors this? Another way to phrase the question is, who reviews and controls the appetite of **Carnivore**? I think that that is really what the purpose of this hearing is.

And as we go into the new arena of privacy, I think we all have to recognize how complex this is in its entirety. And for that reason, I want to finally mention, that there is a privacy commission bill that I've sponsored with Congressman Jim Moran of Virginia, a bipartisan bill that's moved out of the Government Reform Committee, should be coming up on the House floor. But this privacy commission legislation would set up a commission for the first time in 25 years to review our privacy laws. Whenever we had our last privacy commission, we didn't have the Internet. And yet they still called it privacy in the information age. And so I think it's time that we did review this again.

And one of the specific goals and responsibilities of the commission would be to review the activities of law enforcement in terms of privacy and its impact on privacy. So it's not just commercial, but it's also government, it is also law enforcement, a broad-ranging privacy commission. And this is one thing that we can look at not in a reactionary fashion, but in a steady, thoughtful fashion and set the tone as we enter into the next century.

So, with that, Mr. Chairman, I want to again thank you.

I look forward to the testimony of the witnesses.

CANADY: Thank you, Mr. Hutchinson.

The gentleman from Alabama is now recognized for five minutes.

BACHUS: I thank the chairman.

I think obviously what we have here is that technology has outrun the law. We have a Internet explosion, and I don't think the law has kept pace with it. I don't think the laws on the books fit very well with what we're talking about here today.

I have two concerns that I would express to you. One is that we have a balance between legitimate law

enforcement needs and the right of privacy, that we try to maintain that balance, which is a delicate balance.

The second is that we have a balance between our different types of communications. Because if we have certain types of communications where we have the potential to monitor everything that goes through them, but we have other types of communications that we're limited in our surveillance, criminals are going to be the first ones to figure out what is their safest mode of communications. And sooner or later you'll be -- if you have restrictions in one type of communications but not a lot of restrictions in another type of communications, the criminals are going to move to the least restricted or the least monitored form of communication.

And of course we've got to ask ourselves what level of monitoring do we as a country want to have on private conversations, to achieve what level of surveillance?

BACHUS: Let me give you an example. Today -- and this is an example, sort of, quote, "from the old world," but today, coming into this country, Federal Express packages are randomly opened, UPS packages are randomly opened, but U.S. mail is not. I mean, the mail is not opened. Now, criminals have pretty well figured out that the safest way of mailing something in the United States is not UPS or Fed Ex or parcel post, use the U.S. mail. The same going out. They've adjusted. They found out where the loopholes are. They found out where the least surveillance is, and they've gone with using the U.S. mail to send things, because they are not randomly checked.

The criminals are going to figure out, sooner or later, I would think -- and my question to you, aren't they going to figure out -- the illustrations you have given us is that you can take a work like "bomb" and you can search the Internet for bomb. Well, aren't our criminals -- aren't terrorists, for instance, aren't they very quickly going to realize not to use the word "bomb?" I mean, won't they figure out to use the word "dog" as opposed to "bomb"? As opposed to explosive device, won't they come up with some kind of other word? Won't they figure out a way, beyond you using key words, to get around this? And you're basically left on sweeping the conversations of law- abiding citizens? How do you get around criminals who are going to adapt to this system? They're going to be the first to adapt, to learn now to evade this system.

And at the same time my other concern is this: I've heard all sorts of assurances that this won't fall in the wrong hands, that there are safeguards. Well, today there are safeguards on **FBI** files. **FBI** files, only certain people have access to those files. Only certain people can have possession of those files. Only certain people can look in those files. Yet a few years ago, we found out that 1,000 of those files were over at the White House. What assurances do we have that we're not going to have another situation here where we have, like **FBI** files, that they got out of the restricted area and that people viewed them and perhaps utilized them for things they weren't intended to be?

You've read reports, I'm sure, that I have about IRS agents who pull people's income tax forms and they've used them to go up against their wives in court or their ex-wives on child support matters, or they've gone up against someone who was dating their girlfriend to try to embarrass them. And there've been all sorts of reports on what IRS agents did with files or what confidential information, which we were all assured would not fall -- would be restricted, where someone used those files within the IRS to their advantage or to embarrass someone else.

BACHUS: So I would simply say that, despite all the assurances, we know as a practical matter that there're examples, just recently, of restricted information being used for purposes which it was not intended.

So I'd ask you, how would this be any different? How is this any different from IRS information, which we were told would not be disclosed and has been in any number of cases? How is this any different from **FBI** files who found themselves being used for political purposes?

Thank you.

CANADY: Thank you.

We will now move to hearing testimony from our first panel. Our first panel will address the **Federal Bureau of Investigation's Carnivore** program and its role in federal law enforcement in the digital age.

On this panel first we would like to welcome Dr. Donald Kerr. Dr. Kerr is an assistant director of the **Federal Bureau of Investigation** and director of the **FBI's** Lab Division, which develops surveillance and tactical communications technologies.

Next we will hearing from Larry Parkinson, the general counsel for the **FBI.**

Following Mr. Parkinson will be Kevin V. DiGregory. Mr. DiGregory is deputy associate attorney general at the Department of Justice. Two members of the Justice Department's Computer Crimes unit -- Mr. DiGregory is joined at the table today by Christopher Painter, the deputy chief of the Computer Crime and Intellectual Property Section at the Department of Justice. Mr. Painter will not be making a separate statement, but will be at the table with Mr. DiGregory to answer questions.

I want to thank each of you for being with us here today and for patiently listening to our opening statements. I would ask that you do your best to summarize your testimony in five minutes or less, although I don't think anyone will insist on strict adherence to the five-minute rule. And without objection your full written statements will be made a part of the permanent record of today's hearing.

Dr. Kerr.

KERR: (OFF-MIKE) grateful for the opportunity to discuss with you our program for interception, lawful interception, of information on the Internet and data networks.

As you know, the use of computers and the Internet has grown rapidly and has been paralleled by the exploitation of computers, networks and databases to commit crimes and to harm the safety, security and privacy of others. Criminals use computers to send child pornography to each other using anonymous encrypted communications. Hackers break into financial service company systems and steal customers' home addresses and credit card numbers. Criminals use the Internet's inexpensive and easy communications to commit large-scale fraud on victims all over the world. And terrorist bombers plan their strikes using the Internet.

Investigating and deterring such wrongdoing requires tools and techniques designed to work with new and evolving computer and network technologies. The systems employed must strike a reasonable balance between competing interests: the privacy interests of telecommunications users, the business interests of service providers, and the duty of government investigators to protect public safety.

I would like to discuss how the FBI is meeting this challenge in the area of electronic mail interception. In the interests of your time, I've submitted a longer statement, and what I'll do is try to summarize the high points, particularly addressing some of the questions the subcommittee's raised in opening remarks.

First, moving to how we protect the privacy interests of telecommunications users requires me to talk a little about the Carnivore system, what is it, how does it work. Put very simply, it's very much like what some in the networking industry would call a packet sniffer; that is, something able to pick out those packets using the addressing information of the Internet and only those packets to which we've been given access. It works by being placed at a service provider's location in order to get a part of the traffic that's passing through that service provider's portal.

In every case we require a court order. That court order is specific to the numbers we can target, if you will, the addresses we can target, and as to whether it's the equivalent of a pen-register, trap-and trace, or, in fact, full content recovery akin to a Title III intercept.

KERR: To be very clear on the point, we don't do broad searches or surveillance with this system. That's not authorized by a court order and, in my view, could not be.

The way it works, in detail, is that once the court order is issued, the system basically has a filter mask, and that filter mask is prepared with an understanding of the court order so that, for example, the Internet protocol addresses that are the legitimate target of the investigation are called out in the court order and set forth in this filter mask.

Second, we're able to also sort on the "to" and "from" line of the e-mail. And maybe the best way to think about that is think about the piece of standard mail. What it's basically allowing us to do is record the address to which the envelope is being sent and the return address on the outside of the envelope. We're not permitted to read the subject line, and, in fact, do not capture that and record it because we're not authorized to open the envelope with either a pen- register or a trap-and-trace order.

If we have an order that allows us to recover content, we're able to open the envelope. And in this case, what we would then do is capture all of the packets that relate to that e-mail in order to record them on a stable medium -- magnetic tape or some other stable medium -- for later reassembly at another location.

It's installed by a supervisory special agent who has training and experience in, in fact, responding to court orders of this sort, assisted by one of our electronic technicians, and, in every case, by one or more technical people from the Internet service provider.

And I think it's important for you to note that that team of people that records it, or puts the system in place, is not made up of the case agent leading the investigation. This is a technical team of three or more people. It probably also includes an electronics technician from whichever of our field offices is responsible.

We don't look at the text on site until it's recorded and returned, either to a field office or to us at headquarters.

And the installation, to put a picture in your mind, looks very much like a desktop personal computer. It's

often bolted into a rack like other equipment at the Internet service provider location, but an important difference is that it has no keyboard, no mouse, and, in fact, it's locked up, as far as the enclosure is concerned, where the magnetic media are written, because this, in fact, is the first step in the evidentiary chain. And so it's important that it be locked, access only provided to an agent who comes on site to collect the lawfully obtained information and treats it just like we treat physical evidence in terms of chain of custody from thereon.

An important further point is that we produce a record for audit of the filter-setting and the configuration on each installation. In the first few times that it was used, that was done by the people doing the installation. We've now grown concerned, because of discussions that have been ongoing, that we record that in a way so that it's authenticated, and so we now, in fact, override it with a hash, so that if someone tried to rewrite that audit trail, that could be detected.

And that record of filter settings and configuration, in fact, becomes part of the evidentiary record available to the court and the defense as required.

KERR: There are also sanctions for misuse, and no one should forget that. There are both criminal and civil sanctions that cover both Title III and Electronic Communications Privacy Act installations. It's a federal felony, calling for a prison term of up to five years, a fine, plus possible recovery of civil damages.

And so I don't think our technical teams installing these devices are going to risk their jobs, their integrity and their future by attempting to operate this equipment improperly at the ISP.

Moving on to the method by which we respect the business interests of the service providers: every installation has, in fact, been done in collaboration with the service provider's technical staff. To do it efficiently, we, in fact, only want to intercept the very smallest slice of the relevant traffic. And, in fact, where the ISP itself is technically capable of performing the intercept, that is, they have the equipment and the personnel, as many of the large ones do, so they can respond to the court order, we are, in fact, very happy for them to do that and simply provide us the information which is the subject of the court order and we never do install our equipment. We also, in those cases, bear some part of the cost of doing that.

ISPs come in all sizes. I think there are various numbers of them estimated in the United States at the present time, but it's upward of 10,000. They're not all large, listed companies. Some of them are more mom-and-pop operations. They don't have large amounts of equipment and a great deal of technical sophistication. And where the ISP cannot perform in a timely way under the court order, we are then willing to bear the technical and cost burden by installing our system.

Our system is passive on the network. It only receives information through the filter as authorized by the court order and it emanates no signals and no communications over the network. So we don't believe that it in any way would interfere with the proper functioning of the service provider's equipment delivering e-mail to customers.

And, lastly, the equipment is removed immediately upon the expiration of the court order. It does not remain at the Internet service provider, nor is there anyone who can get in and make a decision on their own to leave it in place.

Lastly, does it support us in carrying out investigations in our most important cases? We think it's a well-focused capability. It uses some of the very attributes of the Internet in particular the Internet protocol addressing capability, the "to" and "from" lines of the e-mail in order to restrict our collection to just those who are the targets of the court order. In a sense, it's automatic minimization up front.

Not to say there's not minimization after the fact, because when the messages are reassembled back at the field office or at headquarters, if we have, in fact, incorrectly or inadvertently captured information we shouldn't, it's, in fact, deleted at that time.

And it's really no different than the minimization that occurs first real-time on a Title III wiretap and then subsequent on the recording of that wiretap to be sure there's nothing there that shouldn't be.

It produces evidence with an appropriate first step in the chain of custody. We're trying to maximize the opportunity to properly gather evidence, authenticate it and be able to testify that we've neither added to nor subtracted nor altered that which we've captured.

It's a flexible tool, because it's a combination of software and hardware. And so we can, in fact, adjust it to fit subsequent court orders, and we can move from one case to another with it.

KERR: We maximize the use of commercial software to reduce risk and cost, and as I mentioned before, we've used authentication.

Finally, one of the things we're going to do, as a consequence of our discussion over the last 18 months, with people in industry, staff and members of Congress, five of the Department of Justice components, a number of U.S. attorneys, some 15 federal and state law enforcement agencies, we think it's important to lay to rest this question, Does this thing, in fact, do that which we say it does and only those things which we say it does?

And so we are working right now to undertake an independent verification and validation of the software that we use. We're going to do it with academic members of the team as well as industry members. And by the way, we're not going to contract for those people; they'll be selected by the organization that carries this out for us.

But what we're going to do, is very akin to what, for example, NASA does with software developed for their launch operations: ask some independent party to verify that the software that we have and deploy will, in fact, do those things that we say it will and not provide capabilities that we should not have.

Our year-to-date use of this tool, that is this present year -- the first three quarters of the fiscal year, we've deployed it some 16 times. It's been used six criminal cases and 10 national security cases. Some number of those were simply pen-registers, some involved full content. None of those cases have been adjudicated, so we can't speak to details today, but I think it's probably of interest that it's not a very large number. It is reported in the annual wiretap report in that category called "other," so if you're wondering where the number will found, either now or in the future, that's were it will be.

In summary, I think we've tried to develop a tool, not in advance of policy and precedent, but, in fact, with a great deal of care in understanding the legal authorities under which we are authorized to use this and to target it precisely and well at those that the court orders.

Thank you very much, Mr. Chairman.

CANADY: Thank you very much.

Mr. Parkinson?

PARKINSON: Thank you, Mr. Chairman. I do not have a prepared statement. I'll be very brief.

I want to echo, first of all, what Dr. Kerr said, and this is -- despite its unfortunate name, this is a tool that is very surgical. And I think Representative Hutchison had it right, that this really is a minimization tool. And I'll leave the technical aspects to Dr. Kerr.

What I'm here, primarily, to emphasize -- and I'm delighted to be here and answer any questions that the committee may have -- is to emphasize that there -- the FBI and the Department of Justice have a true commitment to the rule of law. And I want to respond just briefly to the notion that we have deployed this system without controls or without proper authorization. That is simply not the case.

PARKINSON: We are also not saying, Simply trust us, we're the government. I think we have -- we're not naive. We have -- we've had enough situations in the course of our history to know that that's not enough. We have significant oversight, both within the bureau, within the Department of Justice, and most importantly, within the judicial branch that overseas deployment of this device and any other surveillance device.

In addition to that, we obviously have vigorous and appropriate congressional oversight.

So that's why I'm here. I'm happy to answer questions. And I just want to emphasize to you and to the American people that this is a tool that is deployed rarely and it is never deployed without a court order. And we do not deploy it in a way that exceeds the court order.

It is very discriminating, and I hope that this gives us the opportunity to explore that and give some comfort to the committee as well as to the American people.

Thank you very much, Mr. Chairman.

CANADY: Thank you, Mr. Parkinson.

Mr. DiGregory?

DIGREGORY: Thank you, Mr. Chairman.

Mr. Chairman and members of the subcommittee, thank you again for allowing me this opportunity to testify about the law enforcement tool, **Carnivore**, and the Fourth Amendment.

We have seen, as Dr. Kerr has noted, magnificent growth of the Internet over the last 10 years, and it has created vast benefits for our citizens, our businesses and for governments, and it seems to hold boundless promise if we can harness it.

The Internet has spurred a new and thriving economy. Many businesses have prospered by providing their products and services through the Internet. Others have assisted in the building, maintaining and improving the Internet itself. The Internet has given people jobs, supported families and communities, and created new opportunities for commerce for America and for the world. The Internet has touched both our working lives and our family lives.

As we have seen throughout history, however, there are those who would use powerful tools of progress to inflict harm upon others. The Internet has not escaped, unfortunately, this historical truth. Even in the Internet's relatively short existence, we have seen a wide range of criminal use of this technology. It has been used to commit traditional crimes against an ever-widening number of victims.

There are also those criminals intent on attacking and disrupting computers, computer networks and the Internet itself.

In short, although the Internet provides unparalleled opportunities for Americans to freely express ideas, it also provides a very effective means for ill-motivated persons to breach the privacy and security of others.

Many of the crimes that we confront every day in the physical world are beginning to appear in the online world. Crimes like threats, extortion, fraud, identity theft and child pornography are migrating to the Internet.

The Fourth Amendment and laws addressing privacy and public safety serve as a framework for law enforcement to respond to this new forum for criminal activity. If law enforcement fails property to respect individual privacy in its investigative techniques, the public's confidence in government will be eroded, evidence will be suppressed, and criminals will elude successful prosecution.

If law enforcement is too timid in responding to cyber-crime, however, we will in effect render cyberspace a safe haven for criminals and terrorists to communicate and carry out crime without fear of authorized government surveillance.

If we fail to make the Internet safe, people's confidence in using the Internet and e-commerce will decline, endangering the very benefits brought about by the information age.

Proper balance, Mr. Chairman, is the key.

Now, despite the fervor over **Carnivore**, the truth of the matter is that **Carnivore** is, in reality, a tool that helps us achieve this balance.

To satisfy our obligations to the public to enforce the laws and preserve public safety, we use the same sorts of investigative techniques and methods online as we do in the physical world, with the same careful attention to the strict constitutional and legal limits that are imposed upon us.

Carnivore is simply an investigative tool that helps us to investigate online in the same way as in the physical world and enables us to obtain only the information we are authorized to obtain through a court order.

To illustrate: Law enforcement often needs to find out from whom a drug dealer, for instance, is buying his illegal products or to whom the drug dealer is selling his goods. It is therefore important to determine with whom the drug dealer is communicating.

In the olden days of perhaps 10 years ago, the drug dealer would have communicated with his supplier and customers exclusively through the use of telephones and pagers.

DIGREGORY: Law enforcement would obtain an order from a court authorizing the installation of a trap and trace and a pen-register device on the drug dealer's phone or pager.

Now that same drug dealer or kidnapper or a child pornographer may be just as likely to send an e-mail as to call his confederates in today's world.

When law enforcement uses a trap and trace or a pen-register in the online context, however, we have found that at times, the Internet service provider has been unable or even unwilling to supply this information. It is for that narrow set of circumstances that the **FBI** designed **Carnivore.** Law enforcement cannot abdicate its responsibility to protect public safety simply because technology has changed. Rather, the public rightfully expects that law enforcement will continue to be effective as criminal activity migrates to the Internet. We cannot do this without tools like **Carnivore.**

Carnivore is, in essence, a special filtering tool that can gather the information authorized by a court order and only that information. It permits law enforcement, for example, to gather, pursuant to an order, only the e-mail addresses of those persons with whom the drug dealer is communicating without allowing any human being, either from law enforcement or the service provider, to view private information outside the scope of the court order.

In other words, as I understand it, **Carnivore** is a minimization tool that permits law enforcement to comply with court orders, to protect privacy and to enforce the law to protect the public interest.

In addition, as Dr. Kerr has noted, **Carnivore** creates an audit trail that demonstrates exactly what it is capturing.

And as with many other investigative tools, there are many mechanisms we have in place to prevent possible misuse of **Carnivore.** The Fourth Amendment and the courts, of course, restrict what law enforcement can do online with or without **Carnivore,** as do the statutory requirements of Title III and the Electronic Communication Privacy Act.

In the case of federal Title III applications, the Department of Justice imposes its own guidelines on top of the privacy protections provided by the Constitution, statutes and the courts. For example, before **Carnivore** may be used to intercept wire or electronic communications, with a limited exception of digital display pagers, the requesting investigative agency must obtain approval for the Title III

application from the Department of Justice.

Specifically, in the Department of Justice, the Office of Enforcement Operations in the Criminal Division reviews each proposed Title III wiretap application for content to ensure that that interception of content satisfies the Fourth Amendment requirements and is in compliance with applicable statutes and regulations. If the proposal clears the Office of Enforcement Operation, approval must generally be given by a deputy assistant attorney general in the Criminal Division. Typically, investigative agencies such as the FBI have similar but separate internal requirements. If the investigative agency and the Department of Justice approve a Title III request, it still must, of course, be approved by the proper court using familiar but exacting standards.

By statute and internal regulation, the interception may last no longer than 30 days without an extension by the court, and courts also often impose their own additional requirements. In addition, remedies for violating Title III or the Electronic Communication Privacy Act by improperly intercepting electronic communications include criminal and civil sanctions. For violations of the Fourth Amendment, of course, the remedy of suppression is also available.

Despite this panoply of protections, we recognize that concerns remain about this tool. And as Dr. Kerr has noted, the attorney general has asked for an independent review of the Carnivore source code to ensure that its capabilities are what we understand them to be. A report generated from the review will be publicly disseminated to interested groups within industry, academia and elsewhere and should alleviate any concerns regarding unjustified intrusions on privacy from the use of this tool.

Mr. Chairman, my testimony today necessarily highlights a few of the more significant aspects of the balance between privacy and security that the department believes must be struck.

DIGREGORY: The Department of Justice has provided the committee with my full written statement, and it is my sincere hope and expectation that through this and other fora those of us who are concerned about privacy and public safety will recognize that responsible law enforcement can enhance both goals.

Mr. Painter and I are available to try to answer any of your questions along with the rest of the panel.

Thank you, Mr. Chairman.

CANADY: Thank you very much.

Let me say to each of you who have testified that I think your remarks have helped clear up at least some of the questions that have been raised about the system called Carnivore, and I think your testimony has been very helpful to us.

I'm going to have a few questions and other members will have questions. I do want, at the outset, to acknowledge that we probably not get to all the questions that we want to ask, so we would ask you to provide us written responses to any additional questions that any members of the committee may have, but also give you an opportunity to provide any additional comments that you wish to make in light of subsequent testimony that comes in the hearing today.

Let me -- having said that, let me go over some ground that I think you've already covered concerning the use of **Carnivore** under the pen- register or trap-and-trace authority.

When you're using the pen-register or trap-and-trace authority, would you ever obtain any letters or information other than those that make up an e-mail address, such as JohnSmith@home.com? In other words, have you ever or would you ever make a request, under the pen- register or trap-and-trace authority, that included the capture of words or sentences other than the e-mail address?

KERR: The answer from our side in terms of how we set it up is that if it's a pen-register order we only get the two address and we capture nothing else.

PAINTER: And I might say also that the -- even the subject line we consider to be content, and that would require a full Title III. It's just the addressing information and that solely, just as in the telephone context, the numbers dialed, the numbers received.

CANADY: OK. So it's your understanding that your legal authority is limited to the e-mail address, and, of course, it has been your practice -- it is your practice and has been your practice only to obtain the e-mail address when you're using the trap-and-trace or the pen-register authority.

PAINTER: In the electronic communications context, yes, that's correct.

CANADY: Let me ask you this: In your view, does federal law enforcement have the authority under the Pen Register Act to capture so-called URL addresses, which are the addresses of the web sites a person has visited?

PAINTER: If the URL address -- the URL addresses are not really what's contemplated under the pen-register, trap-and-trace statute. What we're talking about there is -- I mean, it could -- it's possible it could be captured if it, for instance, was a Hotmail service. A Hotmail service, as Dr. Kerr can talk about more specifically in a technical way, is a web-based e-mail service, and so you would capture that part of it that identifies is it a Hotmail service and then specifically limits it to a specific authenticating code. And I think Dr. Kerr can talk a little bit about that.

CANADY: If you would.

KERR: Yes, I think that's a very good point. There are services, such as Hotmail, where we have to capture the web page and then look for the authenticators and other indications that it's an e- mail service. Having done that, we limit the collection to simply the e-mail that's provided through that service. We don't capture the users other use of the Internet, we are not interested in what they do when they surf the web, and we restrict what we do only to that e-mail traffic over the web page.

CANADY: OK.

Now, in your comments, Dr. Kerr, you indicated that **Carnivore** has been used only a few times. I think 16 was the number for this year, is that correct?

KERR: That's correct; 16 times this year. I think about a total of 25 in the life of the program over the last

two years.

CANADY: Well, over that same time period, how many Title III intercepts on e-mail would you have done not using **Carnivore?**

KERR: We've used **Carnivore** and earlier versions of the same technology, and in some other cases, we've used a commercial product to try to capture e-mails. And one reason that we moved from the commercial product to **Carnivore,** was, in fact, to get some of the selectivity and audit properties that I briefed you on earlier, because the commercial product had been developed for quite another purpose.

Products like this are used by the service providers to monitor the quality of their service. In that case, they have no legal restrictions on what they can observe. In our case, we're quite limited and need the more discriminating technique.

CANADY: My time has expired, but by unanimous consent, I'll have three additional minutes.

Let me follow up on that, if -- let me change, given the limited amount of time, to a different subject.

How many -- have you contemplated allowing the use of **Carnivore** by other, not only federal law enforcement agencies, but state or local law enforcement agencies?

KERR: At this point in time we have used it on at least one occasion in support of another federal law enforcement agency. We have not yet brought it to the point where we would be talking about it in terms of providing it to state agencies.

As you're aware, the authorities under which they operate are different than at the federal level. And so, we're not necessarily assured at this point in time that it would be a suitable tool for us to turn over.

That said, anytime we turn over Title III or other intercept equipment to state and local authorities, we do so with the signature of the attorney general. She has, in fact, the decision on that; we don't.

CANADY: In my opening statement, I made reference to a media report that Earthlink was required to attach **Carnivore** to its network, in one instance. And doing so, caused part of its network to crash and its customers to lose service.

Now, from your comments, Dr. Kerr, I understand that that just shouldn't happen. I'd like to hear your comments about those reports and what actually took place there and whether this system can pose a threat to the functioning of an ISP, and whether you've had other complaints similar to that made by Earthlink.

KERR: In the specific case, what I will do is try to give you something for the record that's more complete than I can do right now. But initially when we went to Earthlink and they were ultimately compelled to move ahead to do this, they attempted to do it themselves with software that they essentially tried to put together in real time.

KERR: It didn't work and it didn't provide information consistent with the court order.

It's not clear to us that anything we subsequently did had any averse affect on their network. And, in fact, in at least one other case, we've had quite good cooperation from them.

It's the only case where we've, in fact, had to go back and get the judge to emphasize that he meant the order. In all other cases, we've had excellent cooperation, particularly at the technical level and normally at the level of the general counsel of the company involved.

PAINTER: I would add also that in any of these cases, you have to work with the service provider to actually install this. The FBI couldn't go in and just do it themselves. So even when the court orders it, and that happens in each case, you have to work with the technical people to install it.

CANADY: Thank you very much.

Mr. Watt's recognized for five minutes.

WATT: Thank you, Mr. Chairman.

Let me start at a pretty basic level, Dr. Kerr, and pick up on something that you said in response to one of Mr. Canady's questions, having to do with your sharing of this tool with other law enforcement agencies.

And as I recall, your response was that the authorities of the states are different than the authority under which you are operating.

Unless I'm missing something, everybody's operating under the Fourth Amendment to the United States Constitution, so unless you are saying that the Wiretapping Protection Act gives the federal government some additional authority then the states are able to exercise under the Fourth Amendment to the Constitution -- well, maybe I shouldn't speculate about what you are saying.

Tell me what it is you are saying when you say that you are operating under a different authority than the states.

KERR: I would certainly take your point that the states are operating under the same Constitution that we are. But we, in addition, of course, have the Title XVIII statute that guide the federal use of electronic intercept.

WATT: But that's in -- I would take it that that is in furtherance of whatever authority you have as a basic proposition under the Constitution of the United States. It doesn't give you any additional authority, does it?

KERR: No, it certainly doesn't. But the point is that some states, in fact, do not have a statutory basis for state and local law enforcement to do electronic surveillance or they have statutory limitations, all still within the Constitution but, in fact, more restricted or nonexistent in some cases.

WATT: All right. Let me ask another pretty basic question: How long has **Carnivore** or some predecessor form of **Carnivore** been in use by your department?

KERR: Roughly two years. The program began, in terms of a development program about three years ago, but in terms of actual court orders and deployment, over the last two years.

WATT: Square for me, if you would, the notion that you have now engaged in 25 uses of this, 16 of them this year -- or are engaging in them, I guess, on an ongoing basis, because none of them have come to trial yet, and the statement that you made that you are now undertaking or preparing to undertake verification that this system does what you say it does and that only.

WATT: It seems to me that such verification would have taken place at some earlier stage, not 25 cases into public concern or legal concern.

KERR: The essence of the development program, of course, is that you do learn as you develop and deploy. We, as I pointed out, had initially tried to use a commercial product and found that it did not have all of the properties we thought should be in place for long-term use in a law enforcement context. And so we...

WATT: What products -- what properties did it not have that you were looking for?

KERR: It didn't have the same discrimination capabilities. It didn't have the same ability to provide an audit report and report on configuration that we require.

WATT: Now, who is it that -- now that you have the audit capability -- who is that has the oversight in your department to audit what -- to really review the information that you obtain from the audit?

KERR: I think that'll actually happen quite outside of the **FBI** in that the results of the intercept will, in fact, be provided to the court. They will, of necessity, become available to the defense. And consequently, they will be more aggressively questioned, in fact, in that circumstance than they would be in any internal administrative review.

CANADY: The gentleman's time has expired. The gentleman will have three additional minutes.

WATT: Let me turn to a different area if I can. You've compared this to -- the Internet capabilities this -- analogous to a phone tap or the authority that you have to tap phones.

Does your authority to tap phones get you into the internal phone mechanisms of the phone company or is your authority limited to tapping individual phones of individual suspects?

KERR: That's an area that's, in fact, in a state of change today.

WATT: Who's changing it?

KERR: You did, sir...

(LAUGHTER)

... in that the...

WATT: I think I've -- you being Congress, I take it?

KERR: Yes, sir.

WATT: I think I voted against this bill, as I recall, and still have some concerns about it, to be honest with you.

But go ahead, I'm locked with everybody else for that purpose.

KERR: Sorry.

Some of my colleagues know this better than I, but the point is, the Communications...

WATT: Maybe I should be directing this to Mr. Parkinson. He's the general counsel. He should know these things, I guess.

Or Mr. DiGregory. I didn't mean to beat up on the technician here. I'm just...

DIGREGORY: In its most basis sense, as I understand it, the telephone tap is conducted at the phone company but is restricted to the individual line which you wish to tap. Whether you wish to obtain numbers dialed, numbers coming in, or whether you wish to obtain content.

WATT: OK. Now how do you -- how does that compare with the capability that **Carnivore** has for Internet communications?

DIGREGORY: Now, we'll go back to the science side.

KERR: Not to try to confuse you by switching back and forth, but the telephone...

(CROSSTALK)

WATT: I'm pretty confused without you switching back and forth, but go ahead.

KERR: The telephone tap refers to the ability to intercept switch circuits, which was the basis historically of the telephone system. The Internet provides a different kind of technology that we're trying to intercept. It's a so-called packet-switched network. And it doesn't work by my, in effect, leasing a circuit in order to make a phone call from my house to yours, and that's, if you will, for the time of the conversation, our private circuit.

WATT: Let me stop you right there, because my light's going to go off -- has already gone on.

If you needed additional legal authority to get mobile home phone taps, why would not additional legal authority be necessary to -- for you to be doing what you're doing under this system? And maybe again...

(CROSSTALK)

KERR: I'll give you my view and then...

(CROSSTALK)

CANADY: The gentleman has an additional minute.

KERR: ... I'll stand corrected by my colleague.

We do, in fact, have legal authority to do what we're doing today. And I think it's because of the correct belief, from my perspective, that the addressing information on the Internet is, in fact, a useful and appropriate analog to the telephone number in the switch circuit world.

But perhaps, Mr. Digregory or Mr. Parkinson would like to add to that.

PARKINSON: I think that's correct and it's appropriate also to point out that there are gradations of authority, and there's a higher level of authority within the department and a higher level of authority in the courts, depending on what sort of intrusion you're talking about. If you're talking about simply numbers, then we have the pen-register trap-and-trace authority; if you need to go beyond that then we have to move it up a notch or several notches to a Title III authority.

WATT: Thank you, Mr. Chairman.

CANADY: Chairman Hyde?

HYDE: Thank you, Mr. Chairman.

You can understand the skittishness of some people whose concern is privacy. And when you see some of the things that have happened here in Washington, it gives one reason to wonder and to worry.

I speak of the Defense Department releasing an employment application with information that was supposed to be private and it ends up in The New Yorker magazine. And that person -- I think he got a letter, mildly critical of what he did, which doesn't go in his file and no prosecution.

A less compelling case, I case, is over the so-called Filegate where the law wasn't breached at all, but one's sense of privacy was -- took a beating, I should think. And so, there are people who are skeptical about how this culture of privacy -- how porous it is. That doesn't call for an answer, that's just, kind of, a comment.

HYDE: Can you tell us how -- I'll ask this maybe of Mr. DiGregory -- how terrorist cells and organized crime and others use technology and how does **Carnivore** address the growing use of technology by criminals?

DIGREGORY: Well, I think that terrorist cells and organized crime can use the Internet to communicate, can use e-mail to communicate. And simply the same way that a pen register addressed their use of the telephone to perpetrate their criminal activity, **Carnivore** addresses -- or can address their use of the Internet with respect to those activities and obtain, pursuant to a pen-register order, those numbers that are being called by the organized crime figure or the drug trafficker.

HYDE: Could you tell me what reasons you have for not letting the Internet service providers gather the requested information? I take it they have made themselves available to do that for the most part. Maybe some of them haven't. But what are the reasons why you don't let them do it?

DIGREGORY: I don't think it's a question -- and anybody up here is invited to correct me if I'm wrong -- I don't think it's a question of not letting them do it, I think **Carnivore's** use is limited to those situations where the Internet service provider is unable to provide the minimized court-ordered information that the **FBI** requires, pursuant to the order.

KERR: And let me amplify on that a little bit.

The **FBI**, my understanding is, will always allow the Internet service provider to do it if they can, in fact, do it in a timely fashion.

The one time this was actually challenged -- now talking about who the ISP was -- and that one instance the ISP tried to work with their own tool, it was not effective, it was not capturing all of the addresses. It was only capturing incoming and not outgoing addresses. It wasn't giving the whole information. And in that case, the **FBI** was forced to use the **Carnivore** tool.

That is not their first line. The first line is to let the Internet service provider do it if they can. And, in fact, the **FBI** I believe would like the Internet service providers to do it if they can.

HYDE: Fine. Thank you very much. I have no more questions.

I'm through, Mr. Chairman.

CANADY: The gentleman from Michigan's recognized.

CONYERS: Thank you very much.

I think one of the basic questions here is to determine whether or not you're minimizing your activities or whether you're maximizing them. And of course, it's already been asserted that you're minimizing them. And my job is to find out, maybe before the hearing ends but certainly after the hearing, whether that is correct.

And it seems to me that this system that we're oversighting today, unlike other trap-and-trace devices, or the others that we use, is available for -- is subject to the maximization of information, getting more information than is required or is authorized by a court order. And so that's the area that, to me, is very, very unclear as of now.

I'm not sure how we're going to sort this out, but I think we have witnesses here that are going to come forward later on that are going to complain about the fact that there was other information that was available through this system that might not have been available if we weren't going through the Internet.

CONYERS: Isn't that possible, that you can get more information, you can look at other things that would not have otherwise been available?

KERR: One of the points, Mr. Conyers, that I was taking some time with was to try to make it clear that the only information we can capture is, in fact, that specified in the court order. And to go outside of the court order, in fact, is a federal felony with substantial sanctions for those who would do so.

We, in fact, think of this as a tool that's designed explicitly to meet the requirement of the court order. We don't have the authority, nor are our people allowed the opportunity, to step outside of those bounds.

CONYERS: Well, right, that's the law. But, I mean, that's the problem. I mean, if I could be assured that everybody wouldn't do the wrong thing because there was a statute making it criminal, that would reduce a lot of our efforts. And even law enforcement people, I hasten to add.

Mr. DiGregory?

DIGREGORY: Mr. Conyers, as I understand the way the system operates -- and certainly, that's correct, that's what the law is. But there are checks and balances with respect to **Carnivore** which would make it extremely difficult for someone to counter those checks and balances and violate the court order.

It's not just a situation where, as I understand it, a rogue **FBI** agent, for example, could broaden the coverage of the **Carnivore** intercept and violate the court order. In order to do that, he would need to engage the aid of technical people, perhaps even technical people at the Internet service provider, and he would also have to find some way to cover up or change the audit trail that is left by the system so that it doesn't expose his going beyond the court order.

And, again, I'll stand corrected by those who are more expert in the way this system functions, but that's how I understand it. And although, yes, that's the law, there are checks and balances which would make it

extremely difficult for someone to violate the court order.

KERR: And it's also a law we take very seriously. If a law enforcement person violates the wiretap law, they'll be prosecuted. The Computer Crimes Section has a responsibility for doing that and would prosecute particularly law enforcement individuals who violate the wiretap law.

DIGREGORY: And we've done that. Not in the context of these kinds of intercepts, but in the context of telephone interceptions.

CONYERS: So our assurances are that, first of all, there's a law against it which you would assiduously prosecute your own people were they to violate it, and that there are other technological measures that make it very difficult to do anyway. There's a box that actually can search to preclude getting more information than you want. Is that the way I understand that it operates, Dr. Kerr?

KERR: Actually, the way it works is that it's set up in conformance with the order to collect and record that which is part of the order. And in doing that setup and arranging the configuration, the knowledge of that setup and configuration is, in fact, recorded right along with the evidence. Once that evidence is collected, it's, in fact, delivered to the federal court where it's sealed by the judge who issued the order and with an appropriate chain of custody to get it there.

CANADY: The gentleman's time has expired. Without objection, the gentleman will have three additional minutes.

CONYERS: Thank you. I'm not sure if I need them, Mr. Chairman, but let me just say that -- I don't know, maybe the committee is put in a more difficult position than I appreciate.

CONYERS: I don't know if we have any way of verifying that the technological part of the response to my question that you've given me, and I know that, you know, unfortunately in the past, we've had many agencies, including law enforcement, that have gone beyond the scope of their responsibility. There's hardly anything new about that.

So I'm trying to figure out how we're going to get to the bottom of this. We made need a -- we may need technology experts to match yours to verify that what you're telling us makes everybody believe that it's OK, it's the government. And that's what I'm not sure.

GRAHAM: Will the gentleman yield?

CONYERS: Of course.

GRAHAM: I think the gentleman raises a valid point, but I think that that has already been addressed, to a certain extent, by the department's announced plan to have this system reviewed by an independent body of experts who would issue a report that everyone could examine. And I suppose, ultimately, representatives of the independent body of experts could come here to the Congress and answer questions that we might have of them, based on their independent review.

CANADY: Would the gentleman yield from questioning?

CONYERS: Well, yes.

CANADY: Thank you, I'm just concerned about that. Let's assume that an independent body of experts reviewed this system and said it was fine and would do only what it was suppose to do, et cetera, that could change at any time after that. And how would you maintain the trustworthiness that the system was still limited after they had investigated, unless you were going to have an independent group looking over the FBI's shoulder forever? Because obviously you can't trust the police agency forever not to go beyond what they're supposed to do.

CONYERS: Well, I raise this, Chairman Canady, merely to point out that we're, sort of, in the process of taking words for it. And, of course, we're happy to take the government's words, but, you know, this -- as I recall it, Carnivore didn't -- wasn't sent to us, we, sort of, found out about it in the scope of things, and it began to take on a life of its own that led to this hearing.

So I'm anxious to hear from the non-government witnesses to see how their understanding of what has been happening and -- with this system comports with what we're being told. But I thank the witnesses, anyway; that's what your job is about, that's what you're supposed to do.

Thank you, Mr. Chairman.

CANADY: Thank you, Mr. Conyers.

The gentleman from Arkansas, Mr. Hutchinson, is now recognized for five minutes.

HUTCHINSON: Thank you, Mr. Chairman.

On that particular point, you all are willing to submit the source codes to an independent review and audit. I think the dispute is that the ISP community would like to have open access to the source codes for purposes of reviewing it and determining it's authenticity and that it accomplishes what you desire.

What problems would you see, if any, in allowing open access to the source code that make up Carnivore, Dr. Kerr?

KERR: There're two points that we would raise. We wouldn't have any problem releasing it to a group set up to do verification and validation. We would have a problem with full open disclosure, because that, in fact, would allow anyone who chose to develop techniques to spoof what we do an easy opportunity to figure out how to do that.

Beyond that, some of the code we have used is, in fact, commercial off-the-shelf software, and its proprietary to the companies that have developed it, and we're not at liberty to divulge their source code under the license that we've paid for.

HUTCHINSON: So you would be open, though, and it would not compromise legitimate law

enforcement activities, if there was a ongoing review system of the source codes for **Carnivore** or any subsequent adjustments to it.

KERR: I think the only concern we'd have at some point is, you know, when is enough enough? Do you review it each time you set it up for a new case? I don't think that's workable. Do you do it as part of an annual review of electronic surveillance beyond simply counting the occasions when it's in use? That may be more workable.

But clearly, when the number of reviewers are larger than our group that develops the system, we probably have reached some form of imbalance at that point.

HUTCHINSON: Thank you.

Now, let me -- if you have a content court order to use the **Carnivore** system, then, of course, you have to show probable cause, you've got to get your court order. But at that point, is innocent third-party information reviewed by **Carnivore?**

KERR: If we have, in fact, gotten proper information on the target addresses and the "to-from" -- because that's important, too, since more than one person might be using a particular computer -- in principle, we should only get the authorized communication.

That said, if we were to find that we had, in error or because of misinformation, recorded something to which we were authorized no access, we would have to minimize that just as we would on a normal telephone wiretap.

HUTCHINSON: It's been explained to me as a pipe in which **Carnivore** looks at all the data going through the type to seize that which is the subject of the court order.

KERR: Right. In fact, one of the...

HUTCHINSON: Is that pretty much...

KERR: Yes, one of our...

HUTCHINSON: The question...

KERR: ... problems is that the pipes are too big for us to do that and we rely on the service providers to give us just part of the traffic coming through their big pipe.

HUTCHINSON: And I've learned on computers that sometimes delete does not mean delete, that information continues to be stored. And so my question is: Is the information that is not captured pursuant to the court order, is it ever retrievable in any form by any means?

KERR: No, it's not, because it's all in random access memory and volatile memory. So, for example, if the

power goes off, we will lose everything in that memory. None of it gets to the...

HUTCHINSON: What if the power doesn't go off?

KERR: Well, none of it gets to a stable recording medium like magnetic media in a hard drive or a ZIP drive, a floppy disk. Only that which we're authorized and which the filter is set up for gets to that permanent media.

HUTCHINSON: Now, you indicated that year to date Carnivore's been used 16 times, I believe 20 times in all total. How many of these -- of course, these are the ones that's used the Carnivore, is that correct? But you also, in addition to that, use court-ordered wiretaps or pen registers to retrieve Internet information by using ISP capabilities.

KERR: In some of the cases, we've, in fact, been able to ask the ISP and they have provided us the information.

HUTCHINSON: I'm trying to get a contrast. The 16 that you mentioned, were these not by using ISP capabilities? This is when the FBI went in and used the Carnivore system; is that correct?

KERR: That's correct.

HUTCHINSON: All right. So I'm trying to get an idea how many others are out there that were used by ISP capabilities.

KERR: I don't have the number with me. We could certainly provide that to you.

HUTCHINSON: Does anyone know that? I mean, I'm trying to figure out if we're looking at 100 others versus 16.

PAINTER: My understanding for the Title III intercepts is that it is not a large number. Trap-and-trace, it might be a little larger. We can try to obtain those...

(CROSSTALK)

PAINTER: ... Dr. Kerr's indicated -- provide it to the committee.

CANADY: The gentleman's time's expired. The gentleman will have three additional minutes.

HUTCHINSON: Thank you.

I mean, it just strikes me that -- I mean, considering the number of Title III wiretaps of telephone communications, I mean, that's much greater than the 16 or what you've used by ISP. And I guess what I'm leading to is that it looks like, if the bad guys are moving as the whole population is moving to data communications through the Internet, looks like we're missing a whole lot here, that we're really only on

the surface of what we might need to be doing.

KERR: That's certainly true. The tool we've been discussing to this point today, **Carnivore** has, in fact, only been used in the framework of e-mail intercept.

KERR: As you're properly pointing out, there's a lot of other traffic on the network. We continue to work to try to see how we could develop appropriate and lawful tools to go after that traffic as well.

It would tend again to try to use the properties of the network itself; the need for me to be able to move data from my computer to your computer and capture it because of the addressing information that would be there, not by trying to view the content on the fly.

GRAHAM: Would the gentleman yield?

HUTCHINSON: Yes, I'd be happy to yield.

GRAHAM: I don't understand what other kind of traffic you're talking about if it's not e-mail. What realm are we talking about if we're not talking about e-mail?

KERR: Well, one could use other protocols, for example, to move large files, to move imagery, to move larger quantities of data. And it wouldn't move as e-mail in the sense that we've been talking about it today with a, you know, "from me, to you, subject," whatever. It might just move as a block of data. It could, in fact, be information that companies are moving from one location to another.

HUTCHINSON: Have you ever had an occasion to try to retrieve any of that information pursuant to court order?

KERR: We have not had any occasion that I'm aware of where we've tried to intercept that kind of information. In general, large files like that, we would expect to come to rest someplace and we would probably be picking it up as another part of an investigation.

HUTCHINSON: Finally, there's -- looking ahead a little bit, there was a question asked of whether the pen-register orders that are applied to the Internet reveal far more than the numbers that are dialed in traditional telephone wiretaps. And I know that you're restricting it to "to, from" information. You've specifically deleted capturing the subject information because that would be content- oriented.

But this is still a concern. I guess that even the "to" with the address, sometimes a descriptive term -- do you see -- have you, in fact, from your history of the 16 instances that **Carnivore's** been used this year, have there been instances in which you captured more information that you believed you needed pursuant to a pen-register- type capture; that you believed might go into the content area and therefore you had to minimize it?

CANADY: The gentleman -- the gentleman...

HUTCHINSON: I'll just finish this and then I'll be done.

CANADY: Yes. The gentleman's time is expired. The gentleman will have one additional minute.

KERR: I'll reserve the opportunity to answer carefully after review, but there are none to my knowledge.

HUTCHINSON: So in other words, you're saying the system's working. You're not capturing content information beyond that which is intended under the court order.

KERR: That's correct.

HUTCHINSON: Thank you, gentlemen. I yield back.

CANADY: Thank you, Mr. Hutchinson.

The gentleman from New York, Mr. Nadler, is recognized for five minutes.

NADLER: Thank you, Mr. Chairman.

Forgive me if I ask any question that may be repetitive since, because of a plane delay, I arrived late to the hearing.

As I understand it, **Carnivore** can be used either for content or for, in effect, a trap-and-trace, just to know who an e-mail -- who a person is communicating with; is that true?

KERR: Yes, that's correct.

NADLER: So it can be used for either purpose?

KERR: Yes.

NADLER: Or both.

And whether it's used for either purpose depends on the nature of the court order

KERR: That's also correct.

NADLER: And it can be set either way.

KERR: It's, in fact, set specifically to meet the terms of the court order.

NADLER: Now, when you have in effect the trap-and-trace you want to know who someone is talking to; this is for past tense or for ongoing?

KERR: Basically we would capture, under the trap-and-trace and pen-register order, the to and from information. It would be recorded...

NADLER: No, no, is it past tense? You get a court order, we want to know who this guy talked to in the last two months or we want to know who he's talking to in the next two months?

KERR: It's prospective.

NADLER: It's prospective? Now, what is the difference, in terms of what you have to show -- presumably you have to show probable cause that a crime may be committed. Why would you sometimes ask to know only who he's talking to and sometimes what's being said if it's, if they're both prospective?

KERR: I'll let my colleague lead with that one please.

DIGREGORY: It depends upon the nature of the information that you have available to you at the time. You may not have enough information at the time that you seek the pen-register or the trap- and-trace order to establish the probable cause necessary to seek the order -- the Title III order for the content.

NADLER: But you have enough to -- you need a lesser standard of probable cause to get a trap-and-trace?

DIGREGORY: It's not a probable cause standard at all, it's simply a certification to the court by the prosecutor or the law -- and the law enforcement agency that the information that will be obtained through the use of the pen-register and the trap-and-trace -- or the trap-and-trace is relevant to an ongoing criminal investigation.

NADLER: With no probable cause?

DIGREGORY: With no probable cause.

NADLER: So you can get it on anybody with no probable cause?

DIGREGORY: That's correct. And I want to point out to you that this -- that the Supreme Court held, in Maryland vs. Smith, I believe, in 1979, that there was no reasonable expectation of privacy in numbers dialed by a telephone, because, essentially, when someone turns over information to a third party like the telephone company they should not have either a subjective or an objective reasonable expectation of privacy in that information.

NADLER: And does that mean that when I send a letter there's no reasonable expectation of privacy as to whom I'm sending the letter? In the snail mail. Could you get an order to the post office to tell you,

without any probable cause, who is sending me mail or whom I'm sending mail to?

DIGREGORY: We do mail covers all the time, which essentially do that.

NADLER: Without probable cause?

DIGREGORY: That's right.

NADLER: That's very interesting.

Let me ask you a different question.

DIGREGORY: May I just add one more thing, Mr. Nadler? The authority under which we operate is codified at 18 United States Code, I believe it's 31-25 (ph) with respect to the pen -- or 31-23 (ph).

NADLER: Thirty-one-twenty...

DIGREGORY: Twenty-one -- 31-21 at sect, which includes 23, 25, I believe.

NADLER: OK. Now, let me ask you a different question. You installed -- you started using this **Carnivore** system about two years ago, and no one ever bothered telling Congress about it; we just found out about it because Earthlink complained about it.

KERR: Well, no one ever bothered telling Congress in the sense of all of Congress. There certainly have been members and staff briefed on it over the last year. It's been widely...

NADLER: Judiciary Committee staff?

KERR: Excuse me?

NADLER: Judiciary Committee staff?

KERR: Yes. It's been rather widely discussed with industry, Internet service providers, other companies that provide software and hardware to the network. It's been fairly substantially briefed within the Department of Justice, including at the training center in Columbia, South Carolina, where the U.S. attorneys and AUSAs go for training. All of the major investigative programs have been briefed.

NADLER: What institutional safeguards have you set up to make sure that assurances that you've given us that information given by -- gathered by **Carnivore** on subjects not under investigation is not used?

KERR: Every time that it has been used it's gone through the internal review of the **FBI** that all such uses require. My colleague, Larry Parkinson, can speak to more detail on that.

Second, it goes to the Office of Enforcement Operations in the Department of Justice where it's, in fact, reviewed prior to ever going to a court to get a court order. So there's a very substantial level of review internal to the **FBI**, internal to the department, as well as the subsequent review of the court before an order is issued.

NADLER: Subsequent review to the court? I'm sorry.

I think I asked, once you have **Carnivore** on-line, what institutional safeguards do we have that information gathered by **Carnivore**, presumably after the court issues an order to install it, is not misused?

CANADY: The gentleman's time has expired. The gentleman will have three additional minutes.

NADLER: Thank you.

KERR: The answer to that is, that, particularly in a full- content intercept, that the information we intercept and record is provided under seal back to the court, which can itself determine that we've properly followed the order.

NADLER: It's provided back under seal to the court?

KERR: Correct.

NADLER: Is there a proceeding in the court?

KERR: I don't know.

NADLER: I mean, if there's not a proceeding in the court, it'll simply be placed in storage, no one will look at it.

PAINTER: That's not completely true, because it's placed under seal with the court in the Title III content intercept. And then at some time in the future, the court can, under Title III, make that available to, for instance, the person whose conversations were intercepted and/or his defense counsel.

NADLER: Now the person -- if a person has been the subject of such an order and his content has been intercepted or simply -- or simply that whoever he was e-mailing to has been made known to the **FBI**, and it's determined that this person should not be subject to any charges, did nothing wrong, is he ever made aware that his privacy was so violated?

PAINTER: Under Title III -- under the provisions of Title III at -- if a Title III order is denied by the judge or if it expires, after a certain period of time -- I believe it's 90 days -- there has to be notice to the people whose conversations were intercepted. I think that's been done very broadly, as I understand it.

NADLER: So people's whose conversations were intercepted or whose -- or on whose e-mail there was a trace, are eventually told?

PAINTER: Under the provisions of Title III, when you're dealing with content, yes, that's correct.

NADLER: And what about when you're not dealing with content, when you're dealing with a trap-and-trace?

PAINTER: Well, again a trap-and-trace -- and I should emphasize something that Mr. DiGregory said earlier, the trap-and-trace, the reason probable cause is not required, is this is a very preliminary investigative step. It is really, literally, the addressing information and nothing more. And it's...

(CROSSTALK)

NADLER: I understand that, but if you've -- without probably cause to believe that I've committed a crime or done anything wrong, but simply as part of an investigation, you have followed who I'm talking to by e-mail or for that matter, not by e-mail, you put a trap-and-trace on my phone for the last six months, now you've determined that there's nothing further to investigate, do you ever tell me that my privacy was violated in that way? Do I ever know about it?

DIGREGORY: I don't believe that there is any requirement for disclosure in the law. And I would only -- I understand that you're using the term "that my privacy was violated" and only relying upon the case law, which indicates that there's no reasonable expectation of privacy in such information, I just wanted to make that point yet again.

NADLER: Well, that may be from the Supreme Court's point of view, that there's no reasonable expectations of privacy, but I think as a practical matter, most people would be somewhat upset if they thought that someone was following exactly who they were talking to on the telephone or who they were mailing e-mails to.

But be that as it may, from a legal standard that may not be, but the fact is there was -- in a practical sense, there was an invasion of privacy, government gathered information that maybe I didn't want people to know, I think I should know about that. And maybe I should be able to say to the government, On what basis did you do this? Did you have any reason to do it? And maybe they did and maybe they didn't. But right now, there's no provision for that.

PAINTER: Well, that they -- first of all, the prosecutor has to certify to the court that it is relevant to an investigation. And then second, it's that class of information alone, and it's limited to a period; it can't be done ad infinitum. A trap-and-trace order...

NADLER: What period is it limited to?

PAINTER: ... is 60 days.

NADLER: Can it be renewed?

PAINTER: It can be renewed, but it has to go back to court.

NADLER: How often can it be renewed?

PAINTER: I'm not sure there is a limitation.

NADLER: What's the longest anyone has ever been subject to this?

PAINTER: We'd have to look into that to be sure.

NADLER: Has anyone ever been subject for more than, let's say, a year?

PAINTER: Again, I don't have that information available at this point.

NADLER: Five years? Could you rule that out?

DIGREGORY: I mean, I don't -- if you want us to try to find out the longest time that anybody has ever been subjected, we can try to do that. I don't know if we have those records, but we can try to do that.

NADLER: Thank you, Mr. Chairman.

CANADY: Thank you.

The gentleman from Alabama is recognized for five minutes.

BACHUS: Thank you.

The potential for abuse here is tremendous. Would you all agree?

PARKINSON: Congressman, I guess I don't agree with that.

BACHUS: All right. And you don't have to give an explanation.

PARKINSON: Well, I think at a certain point in time we have to rely on the good faith of public servants who are -- who have a number of checks and balances in case they get try to get away with something.

BACHUS: I think you're exactly right. I think what you're saying is, trust us. You have to rely on us.

And what that reminds me of is these IRS agents who used information to check up on their ex-spouses and their boyfriends and their girlfriends and potential adversaries for affections and, you know, all that we've heard for really years and years and years -- J. Edgar Hoover, what he did.

But let's talk about those checks and balances, because I think you're exactly right. I think you have to rely on -- you certainly have to rely on that, because -- you can't go to AT&T today and say, "We're going to analyze all the phone calls that come through your system," can you?

KERR: That's correct. We can't do that.

BACHUS: But you can do that with this -- with **Carnivore**, with...

KERR: No, we, in fact, specifically don't do that. We only...

BACHUS: I know, but you do have to analyze -- or you do have the ability to analyze everything coming through that information stream, don't you?

KERR: No. We, in fact, restrict what we...

BACHUS: Now, you restrict it. But you have the ability to monitor...

KERR: No, we don't. We don't have a system with the capability to do the real-time processing of that much information.

BACHUS: You don't have time -- but you can move it around and just capture whatever you want on that system. I mean, you don't have the ability to go to a telephone...

KERR: We don't have the right nor the ability to just go fishing.

BACHUS: Well, you have the ability to monitor anything within that information stream.

KERR: No, we, in fact, have the lawful opportunity to...

(CROSSTALK)

BACHUS: No, I said you have the ability...

KERR: ... some very specific information...

BACHUS: No, no, no. OK. You might not have the -- you say you don't have the legal ability. But you have the technology to monitor that information stream, anything in it.

KERR: We are not sitting looking at the information stream and moving our filter around. It's, in fact, put in place with a court order. It's not intended...

BACHUS: But you have the technology to go in and monitor every one of those e-mails on the system, if you wanted to. Not all of them at once, but you could just -- you could monitor here, you could monitor there...

KERR: Certainly, if you had access to the system, in principle, you could do that.

BACHUS: Which you do -- and you can't with telephone calls.

KERR: Well, in fact, depending on where you are in the telephone system and what kind of switch you're in, you might be able to do a great deal.

BACHUS: So, you...

KERR: But again, it's the same thing. Remember, the big telephone switches are simply computers as well, and so if you got into one, you presumably could see a lot of traffic.

BACHUS: OK.

KERR: The fact is that there are a lot of bars to our doing that, starting with the law.

BACHUS: Safeguards. They're safeguards.

KERR: What?

BACHUS: They're safeguards. They're safeguards.

KERR: It's the law. It's illegal to do that.

BACHUS: The law. OK. I mean, it's the law. That's one of the checks and balances and safeguards.

KERR: Correct.

BACHUS: Now, one of those was, you said, the Justice Department. You have to go to the Justice Department for -- and notify them and get their approval.

And you said that it takes a higher level of authorities there to get approval for your activities; is that correct?

KERR: What Mr. Parkinson was saying is that for the trap-and- trace and pen-register, which only allows addressing information, it's a different level of review, but to get content where probable cause needs to be demonstrated...

BACHUS: You have to go higher up.

KERR: It, in fact, takes high-level approval in the Justice Department before we are ever able to go to the court.

BACHUS: Well, let me ask you this: Why did Janet Reno not know about this, although it's going on for three years, and she is, in fact, the attorney general?

KERR: Well, I would remind you that the Department of Justice is some 127,000 people...

BACHUS: OK.

KERR: ... and multiple investigations.

BACHUS: No, I think -- I think that's a valid point. There are 127,000 people over there, and we might have...

DIGREGORY: I believe that Attorney General Reno said that she'd known about the capacity to do this. She was interested in taking a closer look at the systems application and implementation...

(CROSSTALK)

DIGREGORY: ... to ensure that we're balancing privacy and law enforcement needs, and I think that's what's going to happen with respect to this independent...

BACHUS: So she didn't about the...

DIGREGORY: ... verification and validation.

BACHUS: How about Echelon? It's our understanding that the National Security Council testified before Congress and said that they routinely shared information they gathered with Echelon to law enforcement agencies. Do they share information with the FBI?

KERR: What you're referring to, of course, is whether the National Security Agency...

BACHUS: I mean, through their Echelon programs, do they...

KERR: Through their various intercept programs may, from time to time, appropriately share information with law enforcement. But there're, in fact, some very important hurdles there, including the Classified Information Protection Act and others, so that, in fact, the primary purpose of a system may have been intelligence collection. Incidental to that primary purpose, it may have collected important information about a crime, either committed or being planned, and there are mechanisms to take advantage of that.

CANADY: The gentleman's time is expired. Without objection, the gentleman will have three additional minutes.

BACHUS: Echelon, as I understand it, they monitor -- they can monitor all telephone calls, all e-mails, all faxes; is that your understanding?

PARKINSON: I think we should defer to the National Security Agency to talk precisely about Echelon. I don't think we're prepared to talk about it today.

BACHUS: I guess I would just ask the FBI. They do share -- you say they -- when he said they routinely shared information with law enforcement agencies, do they share information with the FBI?

PARKINSON: We have, as you probably know, a very significant national security responsibility in addition to law enforcement. So it not uncommon at all for the National Security Agency to selectively share pieces of information that it may acquire. But it does so, as Dr. Kerr pointed out, with significant hurdles and legal constraints.

BACHUS: I think you've raised a good point. I'd like to use that as my final question, and that's -- you say the National Security Council. I think we all presume they're dealing with national security. But then they gain information on another subject. I mean, if it's national security, obviously they could share it with you. But let's say it's another subject. Or let's just say that we're talking about Carnivore -- what's the name of it?

DIGREGORY: Carnivore.

BACHUS: Carnivore, OK. Now the examples you gave us were about espionage or terrorism. But do you use this, say, in antitrust investigation? Would you use it in income tax evasion cases? Can it be used in, say, OSHA investigations, or EPA violations? Are there any restrictions there?

KERR: It would, of course, have to be a federal felony to come under Electronic Communications Privacy Act.

BACHUS: And all those are ...

KERR: And it would have to be, in fact, one of the predicate offenses under Title III to come under those authorities.

So, no, it's not every offense. Clearly Internet fraud would be an appropriate target. Child pornography on the Internet would be an appropriate target. These are major programs within the FBI that we would...

(CROSSTALK)

BACHUS: Can you -- other than e-mail, can you get into files? Can you -- do you have the ability to get into someone's files?

KERR: We have, in at least one case, been able to intercept, using a different protocol -- file transfer protocol, but with relatively small files. We can only get at what we have the addresses for within the protocol that's being employed.

BACHUS: But once you have that and the passwords, you could actually get into maybe a mainframe or someone's database?

KERR: No. We're only authorized what the court order says. It's not a matter of going and doing exploration or surveillance with the tool.

WATT: Will the gentleman yield for a second?

Does that extend to e-mails that have already been transmitted? If you had the address, would you -- would you have the authority and/or the capacity to go in and either look at the content of a prior e-mail or look at the number or instances in which there has been communication to deliver that e-mail?

CANADY: The gentleman's time has expired. The gentleman will have one additional minute.

BACHUS: Thank you.

Let me -- after he answers it, may I have my minute then?

KERR: Shall I try to answer Mr. Watt's question?

BACHUS: Answer his, yes.

KERR: OK. The **Carnivore** system basically deals with message traffic on the fly. If the messages have already been sent and received, another way we, for example, might get it would be if, for example, a search warrant were offered and we seized a computer and we found the messages on the hard drive of that computer. Or, as one of the members of the subcommittee pointed out, deletion doesn't necessarily mean deletion. We can, in fact, sometimes recover messages even though they have been thought to have been deleted. And we have a unit that does that. But they work under a more normal search warrant environment.

DIGREGORY: And under certain circumstances, stored communications that are held -- stored e-mail communications held by ISPs can be obtained by search warrant as well.

BACHUS: All right. Here's my final minute. You mentioned...

CANADY: The gentleman will have one additional minute.

BACHUS: You mentioned judicial oversight. And, Dr. Kerr, you mentioned that you've got the defense attorney and he's looking over our shoulders; you have the judge, he's looking over our shoulders. And obviously if the defense attorney has the ability to do that, that is a pretty potent weapon in limiting what you do.

But are you saying, when you say that, that all these cases are ongoing criminal cases in court where there is, in fact, a defense attorney? Or could it be -- what about a case of an investigation where there's no attorney or not active court case?

KERR: I think Mr. DiGregory pointed...

BACHUS: Or can it be used in those cases?

KERR: ... out the provisions of Title III that would lead to judicial notice of those who had been intercepted. They certainly, at that 60- or 90-day point, having been informed that their communications had been intercepted, would take a great interest, with or without their attorney, so I think that the system is oriented very well to protect their privacy and rights.

BACHUS: Are you unable to take information you gain from these investigations and pass them on to other law enforcement agencies about unrelated investigations? Or is that information off limits?

CANADY: The gentleman's -- I'm sorry, the gentleman's time has expired. The gentleman's had more time than anyone else. We're going to go to -- we have a limited amount of time. The members of the panel can answer a written question about other things the gentleman might want to ask, but Mr. Barr's entitled to have his time.

So Mr. Barr is recognized.

BARR: Thank you, Mr. Chairman.

This is actually quite fascinating. The Clinton administration is fascinating. It never ceases to amaze me. For over -- for almost a year now at the other end of this very hallway, in the Government Reform Committee, we've been having a series of hearings, the conclusion of which, from the Clinton administration standpoint is, we don't even know how to keep track of our own e-mails. And now we have a very sophisticated system for tracking other people's e-mails.

BARR: The fact of the matter is, I think they know exactly what has happened to their e-mails and they know exactly what's happened. I just think that we have two different directions for the Clinton administration: When they want to protect themselves, they have one standard; when they want to get information out of other people, they have quite a different standard.

And the fact of the matter is, with all do respect, simply because there is a privacy act or simply because there are sanctions in Title XVIII for misuse of the Title III provisions does not guarantee that nobody in this or any other administration will abuse it. So I think we really need a little bit more than simply saying that there are provisions in the code.

The problem that I have with Carnivore, several problems, but the fact of the matter is Carnivore is not a passive system: It doesn't sit there like a basket and these e-mails just sort of drop into it. It is very much an active system. And it has to have some mechanism for scanning the information in that ISP stream in order to pull out what the court order allows you to pull out.

The problem -- let me ask about two things, though, that are particularly problematic. As you all have testified earlier, with regard to Title -- Chapter 206 of Title XVIII, which are all of the provisions that we've been talking about that govern trap-and-trace and pen register, you're doing something very different here, and that bothers me.

With traditional trap-and-trace and pen registers with phone numbers, as you all have testified, you get an order -- granted the threshold is substantially lower than a Title III and we understand that -- you get that from a court -- a court has to grant it, there's no discretion for the court -- and the telephone company, as it were, has to comply with it. They can't say -- they can't just, you know, give you the high-hat and say, "We're not going to do," they have to comply with it. And you tell them what you want and they give you what you want. And if they don't then you can bring sanctions against them, because they are required under the statute to do that. You're doing something very, very different here.

What you're doing here is, you're going to that ISP provider, which stands in the shoes of the traditional phone company when you're looking at a traditional hard number trap-and-trace or pen register, and you're saying, We're not satisfied with what the statute says that you have to install this and give us the information. We don't trust you. I don't know why you, you know, what your rationale is, but you're saying, What we're going to do is, we're going to go outside of the law here, basically, and we're going to force you to allow us to put our software into your system. You will not be able to monitor it. It's completely unsupervised and we're then going to take it from there. Thank you very much guys; you just give us access and we'll do our thing. That's very different from the way trap-and-trace and pen registers work under the traditional Chapter 206 scheme.

Also -- I think also, there is new legal ground that you all are trying to break here and establish the precedent that I don't think is existing anywhere in federal law or case law -- now, I know you're trying to make it in the Earthlink case -- where you're saying you have the authority to go in and, sort of, harvest large quantities of information and you'll filter out what you want.

I think those are two very, very large steps that we're taking here. I don't think this has been well thought out. And that's two areas that I have concern about. Why is it not sufficient -- because we have both testimony, as well as a number of articles that indicate that Internet service providers have indicated, and I haven't seen anybody refute it, that they can do the very same thing that Carnivore does, but do it in a much -- in a way that is much more protective of the privacy of the Internet service provider users.

And, certainly, if you would go to Earthlink, for example, and say, "This is the information we want," the same as you would do with the phone company for a trap-and-trace or a pen register, they're obligated -- they would be obligated to give that information to you, and if somehow you had evidence that they were not doing it or that they were not capable of doing it, and I don't think that's the case, then you could seek sanctions against them.

Why is it, in both of these areas, you're trying to break new legal ground?

BARR: What is it that's insufficient that you don't like about the existing statute that you're willing to operate within the bounds of it?

PAINTER: Let me answer with respect to that last point whether or not there's been cases where the Internet service provider could not provide the information, and Dr. Kerr can talk about this as well.

There have, in fact, been cases -- in one case, without mentioning who the provider is, in fact the Internet service provider was not able to provide all of the information. In that case, in fact, it wasn't just a matter of them saying, Well, we have to comply with a court order. They went back to the court, there was a proceeding before the court, all of these issues, including the issues about too much material being grabbed by this program -- or that was at least the argument that was raised -- were raised with the court and the court ordered this device be put in place.

BARR: And that was not the Earthlink case?

PAINTER: Again, since that was an ongoing criminal case, I don't want to mention who the Internet service provider...

BARR: Well, let's not play niceties here. I'm asking, was that the Earthlink case, because that's been reported in the newspaper, it's not some great dark secret. And I think you are describing the Earthlink case.

PAINTER: I think the problem is this is an under-seal proceeding, there is a court order in that proceeding, I don't want -- because it's an under-seal proceeding we could talk about the public facts that were argued at the hearing, but I don't want to mention the name of the provider.

BARR: I thought you said at the beginning it wasn't the Earthlink case.

PAINTER: I did not say that. I said I don't want to...

(CROSSTALK)

BARR: I think it is.

PAINTER: But in fact...

(LAUGHTER)

PAINTER: But in fact, in that case, there was not complete information given because only the outgoing -- or the incoming messages were trapped but not the outgoing messages, and there was some evidence to

that effect that was presented to the court in the form of affidavits...

(CROSSTALK)

BARR: But that's very different from the testimony that we've had from Earthlink.

PAINTER: And what I was going to say is it's certainly the policy, as I understand, at the FBI and the preference that if, in fact, the Internet service provider can provide that information and do it in a timely fashion, that's what they'd prefer. It raises this sort of example.

CANADY: The gentleman's time has expired. Without objection, the gentleman will have three additional minutes.

BARR: Thank you.

Are you saying, then, that in every one of the 25 cases in which Carnivore has been used, the only reason that it has been used is the Internet service provider has told you they cannot provide the information that you need?

PAINTER: That is my understanding, and I defer to Dr. Kerr to also address that.

KERR: I think that that's generally the point. In fact, our favorite outcome is that, if the Internet service provider can, in fact, provide the information to us covered by the court order, that that's what we would like to do. And there's some very large Internet providers not too far from here,who have the entire capability to do that.

At the same time, in some of the over 10,000 ISPs around the country you'll find some that have very limited technical capability, their capital structure is very small, they're not in a position to buy equipment and set up a capability for us that may only be used once in the entire business history of that company. In those cases where they can't preform, we're prepared to take the technical and cost risk away by bringing in our Carnivore system and employing it.

BARR: Here we go again. I guess what you're telling us is Carnivore's, sort of, the privacy advocate's best friend, that it, you know, hey, we -- I mean, do you have ISPs breaking down your door and saying, "Please install Carnivore"? I don't think so.

Is there any specific statute or case law, other than perhaps the Earthlink case, which is currently pending as I understand it, that provides authority for the government to go to a provider of electronic information, a telecommunications firm, and say, "Give us everything you have and we'll filter out what we have"?

That's very different from the traditional rationale underlying both Title III and Chapter 206, which is the government can't go in and just harvest everything on its own and then filter it out; you tell somebody exactly what you want and that's all that you get.

DIGREGORY: In the case to which -- in the case referred to by Mr. Painter, we successfully relied upon

the pen-register statute. And know of -- and I stand corrected if someone has a correction to make -- and I know of no other case where an ISP has challenged our reliance on that statute.

BARR: No, but is -- what I'm saying is, is there any statute or case law other than this one case, that as I understand it is still in litigation?

DIGREGORY: And I'm saying we've relied on the pen-register statute successfully in this area...

(CROSSTALK)

BARR: So you -- the Department of Justice...

(CROSSTALK)

DIGREGORY: ... and there have been no other challenges other than the one mentioned by Mr. Painter.

BARR: The Department of Justice position is that Chapter 206 provides statutory, therefore, also constitutional authority, I guess you would argue, that you had -- that the government has the authority -- the right to go in and harvest a large category of information, far beyond simply the target, and then itself take out the targeted information.

CANADY: The gentleman's time has expired. The gentleman will have one additional minute.

PAINTER: I think when you use the term harvest, you're using a term that really doesn't apply here. That's not what it's doing. It is only harvesting, it is only capturing the information specifically that you allow and the court order has mandated.

BARR: But in order -- I mean, this is sort of -- that's what I love about the Clinton administration, then you get into this circular argument, it's almost metaphysical. You have to have some way of going in there and finding what you're looking for, otherwise it's a non-sequitur.

KERR: Let me, as the -- part of the non-political agency here, try to answer your question directly. What do we actually do in the **Carnivore** system?

What we do is, we first ask the ISP to bring us the smallest part of the message traffic that would contain the target messages. We then bring it to an interface, where, in fact, a clone of that reduced set is made. The regular message traffic goes on, unimpeded, to the legitimate recipients of it. We then filter the cloned stream of information and the packets that do not pass our filter, because we're not allowed to record them, in fact, vanish at that point. The only thing that passes our filter are the packets with the appropriate addressing information to meet the court order. And I think we've demonstrated that a number of times.

In fact, we appreciated your visit, some months ago, when you saw it. As to...

(CROSSTALK)

BARR: When I saw what?

KERR: When you were at Quantico, some of the demonstrations we gave you, were, in fact, of these capabilities.

BARR: That was years ago. That was on CALEA. That was like, four or five years ago, that had nothing to do with **Carnivore.**

KERR: Well...

(CROSSTALK)

BARR: Well, I hope it didn't, because it wasn't described to me as **Carnivore.**

KERR: Hadn't been named yet, perhaps.

But the point is that we're not scanning the full message traffic passing through an ISP. In fact, to do it effectively we want to use the smallest subset of that. A very sophisticated, larger ISP will, in fact, give us the ultimate subset, which is the target messages, and we would have to install nothing.

In some cases, we have to provide technical assistance by putting our system in the ISP in order to do that final filtering.

CANADY: The gentleman's additional time has expired.

I want to thank all the members of this panel for your testimony. I think we've had good presentations in your testimony. And the questioning period has been, I think, very helpful.

We will have additional questions, as I indicated in the outset, and we will do our best to send those to you very soon. And I would ask that you do your best to respond to us within a very short period of time after you receive the letter of which we will send with the questions. Again, we thank you for your testimony and your assistance to the committee in this oversight responsibility.

And now we'll move to our second panel. And I would ask that, as people are exiting the room and coming into the room, to try to be as quiet as you can, because I'm going to proceed with the introduction of the members of the second panel as they are coming forward to take their seats.

The witnesses on this second and final panel of today's hearing will discuss privacy concerns and concerns for network security raised by the use of **Carnivore.**

Our first witness on this panel will be Barry Steinhardt. Mr. Steinhardt is the associate director of the American Civil Liberties Union.

CANADY: Next we will hear from Alan Davidson, who is the staff counsel for the Center for Democracy and Technology.

Following Mr. Davidson, will be Tom Perrine. Mr. Perrine is a principal investigator for the Pacific Institute for Computer Security. He is also the manager of security technologies for the San Diego Super Computer Center.

Robert Corn-Revere will then testify. Mr. Corn-Revere is an attorney at Hogan and Hartson, specializing in First Amendment, Internet and communications law. Mr. Corn-Revere is also the co- author of a three-volume treatise entitled, Modern Communications Law. We have heard from Mr. Corn-Revere on this subject previously.

Following Mr. Corn-Revere will be Matt Blaze, a research scientist at AT&T Labs. Mr. Blaze specializes in the architectural aspects of security and trust in large-scale computing and communication systems.

Stewart Baker, an attorney at Steptoe and Johnson, will then testify. Mr. Baker represents major telecommunications equipment manufacturers and carriers in connection with the Communications Assistance for Law Enforcement Act and law enforcement intercept requirements. Mr. Baker was the general counsel of the National Security Agency from 1992 to 1994.

Finally, we will hear from Peter William Sachs. Mr. Sachs owns ICONN, LLC, a small Internet service provider based in New Haven, Connecticut.

I want to thank each of you for being with us here this afternoon. I would ask that each of you do your very best to summarize your testimony in no more than five minutes. Without objection, your written statements will be made a part of the permanent record of today's hearing.

So we will now turn to our first witness of this panel, Mr. Steinhardt.

STEINHARDT: Thank you, Mr. Chairman.

I want to thank the committee for the opportunity to speak here today. I'd also want to thank you for so expeditiously calling this hearing.

As I think the prior testimony made clear, we are dealing with an extremely important issue, and one that bears a great deal of scrutiny, more scrutiny than even this hearing will allow for.

Let me begin to put **Carnivore** into some context. To my knowledge, **Carnivore** is unprecedented in the history of domestic communications surveillance. Never before has law enforcement installed a device which accesses all the communications of a service provider's customers, rather than only the communications of the target of a particular order. Never before has a law enforcement agency claimed that it should be granted access to all communications passing through a service provider's network based

on an unsupervised promise that it will not stray beyond the confines of its authority.

Carnivore is roughly equivalent -- as a number of the members have suggested, it's roughly equivalent to a wiretap, capable of accessing the conversations of all the phone company's customers or to use the analogy that was offered before, when it suggested that the to and from which the **Carnivore** box uses as the key to look for which messages to record, the analogy of a letter, this is the equivalent of going to a post office and stationing an **FBI** agent there, looking at the addressing information of every letter that goes through and then picking out those which it wishes to record either the addressing information or to open up and actually look at the content.

Now I must say, I want to comment on one thing in this section -- one thing that you were told about earlier this morning, and that's this audit trail that for the first time we've heard about -- this audit trail which apparently we are told records at least what the filter settings are and some of the traffic information.

I think there are probably a number of things that are worth noting about this audit trail. First, this apparently was created only recently, and I would suspect created only after the public disclosure and discussion of **Carnivore.** But, secondly, I think it's worth noting about the audit trail, is that it's only of use in a very limited number of cases, that it really provides very little in the way of assurance.

It's, for example, not available in cases where there is a trap- and-trace or pen-register order. Who is going to look at this? They're not required to turn over even the audit trail to a judge.

It is, as a number of the members suggested earlier, not particularly helpful if the conversations or the addressing information that has been recorded -- picked up, is of an innocent third party, not the subject of the order, not someone who's being prosecuted.

STEINHARDT: They don't have a defense attorney, they don't have an opportunity in which to contest that. I think that what the discussion about the audit trail suggests is that you need to look very, very carefully at all these details.

It's hard to imagine how the operation of Carnivore can be squared either with the Fourth Amendment or ECPA, which was adopted to implement the Fourth Amendment in the context of electronic surveillance.

The very premise of the Fourth Amendment is that searches should be narrow and targeted so as to avoid the intrusion into the privacy of persons who are not engage in a crime or for whom law enforcement does not have reasonable cause to believe that they are engaged in a crime.

In recognition of this, ECPA requires the government to specific the person who's the target of the investigation, crimes under investigation, the particular systems from which the communication is to be accessed. They place on the provider of the communications medium the responsibility to separate out the communications of persons authorized to be intercepted from other communications.

Law enforcement is required to minimize the inception -- the interception of non-incriminating communications of a target of a wiretap order. **Carnivore** is not a minimization tool, as been suggested. **Carnivore** is in fact a maximization tool because it is capable of giving law enforcement access to the entire stream of communications that is traveling through the service providers' networks.

Now, I think it's fair to say -- and I urge you not to take the leap today to think that this is a settled question. I think it's fair to say that the Congress never contemplated or authorized a wiretapping scheme that allowed law enforcement to access everyone's communications, that had the potential to access an unlimited number of communications, only a small fraction of which involve criminal activity, and that targeted entire communications network rather than a particular person's communications.

The questions Mr. Barr asked are exactly the right questions. What is the statutory authorization for **Carnivore**? What in the statute, what in ECPA, what in the Constitution gives law enforcement, gives the **FBI** the authority to insist that a service provider install **Carnivore**? I think that's an extremely important question which is not answered by one case, which we know very little about other than the back and forth in the public and to some extent before this committee -- that we know very little about and that never went higher than one federal magistrate.

Now, the **FBI** has two responses to the concerns that have been raised by **Carnivore**. First, they assure us that they can be trusted to strictly adhere to the Constitution and statutes. Second, they argue that they're being hamstrung by new technologies and that **Carnivore** is necessary to conduct successful investigations. Let me first address the "trust us" argument.

The FBI has a very checkered past when it comes to fidelity both to the Fourth Amendment and First Amendment rights of Americans. As a number of you pointed out, we all know about the wiretapping of Martin Luther King and other leaders of the civil rights movement and the more recent cases where there has been illegal surveillance of political figures.

But even if you assume, for the sake of argument, that **FBI** officials, **FBI** agents are not going to engage in a bald criminal violation of law, I think you need to look at the recent history of the **FBI**, which tells us that -- the recent history tells us that the **FBI** cannot be expected to keep its promises on communication surveillance history. Recent history tells us that we can fully expect the **FBI** to push the envelope of the wall -- as they have done in this case by pushing the envelope of the trap-and-trace laws, for example, to claim that **Carnivore** is a permissible result -- and to eventually break out of the envelope of the law.

Let me give you -- let me give you some examples.

I think best example -- and I detail this in the appendix to my testimony, I go through a good deal of this history, but let me give you one example. When Congress passed the Communications Assistance to Law Enforcement Act that was referred to here earlier today, CALEA, in effect a bargain was struck: In return for requirements that new networks be constructed to preserve the then-existing capabilities for law enforcement, law enforcement, the **FBI** in particular, agreed not to use the new law to force service providers to provide it with new surveillance capabilities or with greater capacity than then existed.

Simply put, the **FBI** has not kept its end of the bargain. The CALEA implementation process has been characterized by an **FBI** power grab. As I detailed in my -- in the appendix to my testimony, the **FBI** has consistently sought greater capacity and new surveillance features than existed in 1994. In some cases it has sought capabilities that were specifically promised to the Congress that they would not seek.

Now, I will only given one example of this. Others are in my testimony. But I think this example is worth fastening on for the moment.

When CALEA was considered, the FBI explicitly told the Congress it would not use the new law to seek to turn cellular telephones into location tracking devices.

STEINHARDT: Director Freeh testified that, quote, "There is no intent, whatsoever, with reference to this term" -- parenthetically this term meant call set up information -- "to inquire anything that could properly be called tracking information."

Well, whether or not that was Director Freeh's intention in 1994, it quickly became the FBI's policy in 1995. And the FBI has fought tooth and nail -- first with the cellular telephone industry, then with -- before the Federal Communications Commission, and now in the U.S. Court of Appeals for the District of Colombia, fought tooth and nail for the proposition that CALEA, in fact, does require the cellular operators to provide it with location tracking information.

Now, on the question of the supposed new circumstances that require Carnivore, first, you're going to hear testimony from the Internet service providers here today and you've already heard a good deal from them in the press, that they are willing and able to provide law enforcement with a narrow targeted set of communications to which law enforcement is entitled.

They can perform the segregation of communications that is the equivalent of providing access to dedicated line; there is no need to resort to Carnivore. And I urge you not to simply trust on faith the suggestions of the witnesses that you -- that you heard earlier today, that there have been cases that other service providers cannot provide them with that information.

Once again, we're in the position of, "Trust us, we know how this black box works," or in this case, "We know that the service providers cannot give us this information without resorting to this black box." The only case that we know anything about in detail, and not many details, because these matters are all under seal, because these cases all come up ex parte -- these request for orders come up ex parte, is Earthlink.

And it was quite clear this morning -- this afternoon, rather, that the witnesses from the government were not prepared to ask you to do much more than trust us, there are cases.

CANADY: Mr. Steinhardt, you're now at 10 minutes. So if you can conclude, because -- let me just explain to all the members of this panel. This subcommittee has another hearing. That's not minimizing the importance of this in any way, but we do have a hearing on a proposal that Mr. Frank has introduced, which we are moving to after this.

So to the extent that you can really stay close to that five minutes, it would be beneficial, given the size of the panel.

FRANK: Mr. Chairman?

CANADY: Yes?

FRANK: Is it the intention of the chair to adjourn this hearing and go to the next one at 4?

CANADY: It is the intention of the chair to hear the witnesses and to have one round of questions, and then go to the next hearing.

FRANK: Thank you.

STEINHARDT: Well, I'll stop there, and allow the rest of the panel to speak, then.

CANADY: Thank you, Mr. Steinhardt.

Mr. Davidson?

DAVIDSON: Hi, I'm Alan Davidson, with the Center for Democracy and Technology. I'd like to thank the committee for holding this hearing, and commend you for your continued thoughtful exploration of the Fourth Amendment and cyberspace, a very important issue today.

CDT is a civil liberties group, and we're concerned about **Carnivore** for at least two reasons: first, because **Carnivore** itself, as it's implemented is very problematic; and, second, because **Carnivore** raises broader issues about the need for greater privacy protections in our increasingly outdated statutory and constitutional framework that governs our surveillance and privacy laws.

Just to start with the first, the questions about **Carnivore.** I think the threshold question for **Carnivore** is that it has -- **Carnivore** has access to much more information than it is legally entitled to collect. How do we know that we can trust **Carnivore?** How do we know what kind of leash has been put on **Carnivore?**

I'd like to, with the committee's indulgence, try to give the committee a sense of a little bit of what we're talking about with packets, here. I've got a couple of slides that I'd like to put up quickly.

Let me just give a couple of disclaimers. These are captures of actual real packets. And for those who didn't bring their opera glasses, these are actually -- should be in your packets. They're the -- and for folks in the audience -- they're the last three pages of my testimony.

These are examples of real packets that have been captured from CDT's network with a very crude tool. That's a tool that may not look anything like what **Carnivore** looks like, but I thought it'd be helpful for the committee to at least get a sense of what some of the things that we're talking about look like and how hard it is to do some of the things that **Carnivore** says it's doing, and how hard it is, maybe, to trust **Carnivore.**

DAVIDSON: And to start with, this first packet is a sample e- mail message -- actually a real e-mail message that I sent to Paul Taylor, subcommittee counsel, on Friday and was captured off of our web site -- off of our network.

What's interesting -- this is what a packet sniffer does to a packet. It, kind of, breaks it up into different pieces that can be understood. And there are, sort of, really -- sort of two chunks to this information. The first chunk is the stuff at the top, which a lot of people call the header information, which contains a lot of the addressing information and description of the packet. The second half of it is what I call the data part, or the payload of the packet. And that includes the data, the text, the content, if you will, of what we're